WEST

Help Logout

Main Menu | Search Form | Result Set | ShowS Numbers | Edit S Numbers | Referring Patents

First Hit | Previous Document | Next Document

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC

Document Number 1

Entry 5 of 5 File: USPT Jul 31, 1984

US-PAT-NO: 4463250
DOCUMENT-IDENTIFIER: US 4463250 A

TITLE: Method and apparatus for use against counterfeiting
DATE-ISSUED: July 31, 1984

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
McNeight; David L.	Tarvin, Cheshire	N/A	N/A	GB2
Lawrence; John G.	Wilmslow, Cheshire	N/A	N/A	GB2

APPL-NO: 6/ 380713
DATE FILED: May 21, 1982
FOREIGN-APPL-PRIORITY-DATA:
FOREIGN-PRIORITY:
FOREIGN-PRIORITY-APPL-NO: GB 8121469
FOREIGN-PRIORITY-APPL-DATE: July 11, 1981

INT-CL: [3] A63B 71/06
US-CL-ISSUED: 235/385; 235/383, 235/375
US-CL-CURRENT: 235/385; 235/375, 235/383, 283/70
FIELD-OF-SEARCH: 235/379, 235/375, 235/376, 235/383, 235/384, 235/385, 235/380, 340/825.36, 340/825.34, 340/825.54, 364/403

REF-CITED:

U.S. PATENT DOCUMENTS

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
4120452	October 1978	Kimura et al.	235/381
4191376	March 1980	Goldman et al.	235/385
4340810	July 1982	Glass	235/375

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY
0006498	January 1980	EP
1519256	July 1978	GB
1536372	December 1978	GB
1554585	October 1979	GB
2052819	January 1981	GB

ART-UNIT: 214
PRIMARY-EXAMINER: Pellinen; A. D.
ASSISTANT-EXAMINER: Lev; Robert
ATTY-AGENT-FIRM: Oblon, Fisher, Spivak, McClelland & Maier

ABSTRACT:

A method for use in the detection of fake mass-produced articles that may

It should be emphasized that the UET card is capable of interfacing with a variety of mainframe computers for special applications such as medical cards, drivers license identification cards, etc. The transactions for which the UET card is used take place electronically in real time, including issuing a card. The transactions are recorded electronically and do not need paper receipts either at the customer end or at the credit card company end. It is also possible to provide on line analysis service from the main central computer to the UET Card holder for credit verification, transaction analysis, billing, payments, etc.

FIG. **3** is a block diagram of the major components of the UET card of the present invention. In the preferred embodiment, the UET card includes a full scale LCD & touch screen display **30**, although the display can be a smaller size, so long as it is large enough for the messages displayed on it to be readable by a user and so long as it is large enough to enable a user to operate the touch controls discussed herein. The UET card also includes an associated display controller **31**, a micro controller along with RAM/ROM/and Input/Output port management **33**, a non-volatile RAM **34** and or touch memories with direct contact to connect to the CIU, a light emitting diode **35** to indicate the status of on/off switch **36**, a speaker/beeper **37**, pin contacts **38** to connect to the memory and to charge the battery, infrared or radio frequency option to communicate and, a built in rechargeable or ordinary batteries **30** to power all electronics for the card.

The UET Card is an active device with a display which is large enough for the user to view information relating to the "credit card" to be used in a transaction, the details of the transaction, and the other information described herein. The memory must be of sufficient size to store a predetermined number of different cards and transactions. The main purpose of the UET Card is to consolidate variety of plastic cards in one and to eliminate paper transactions by storing all transactions in the card memory, which can be down loaded to the home PC.

FIG. **4** is a diagram of the major software blocks which may be used in the UET Card. The software blocks include a database which may include, for example a 32 bit—non erasable unique number **401** assigned to each UET Card for security; a primary credit card issuing company or service institution number **402** which includes information about service institution, such as the name, address, telephone number, etc.; personal data **403** such as name, address, telephone number, fax number, office address, phone number, height, weight, birth date, social security number, blood type, marriage status, and other appropriate information; credit card account information **404**, such as American Express, Visa, Diners Club, containing data similar to that stored in present plastic card magnetic strips along with the visible information on the cards, bank cards **405**; ID cards **406**, including photographs of the user, fingerprints or other forms of identification; health cards **407**; or any other cards **408**, such as, travel, car rental, specialty shop, or restaurant cards.

It should be emphasized that the primary credit card issuing company provides the first hardware/software and all the necessary interfaces to the customer. Thereafter secondary card issuing companies will issue new cards by writing electronic prints by dialing in to the card along with appropriate customer and card issuing company information.

Corresponding to each card, a data area **409** is provided for transient information related to the date of issue, date of expire, credit limit, etc. This can be charged periodically by the card issuing company. Also corresponding to each card, a transaction memory area **410** is provided to store all transaction receipts in electronic form to eliminate or reduce paper receipts. The transactions can be down loaded to a home/office PC. In addition, transactions are also stored in the main central computer of the card company.

The UET Card software also includes an operating system **412**, memory management **413**, database management **414**, display formats and associated management **415**, analysis algorithms and procedures **416**, and a CIU and PC interface **417**. In addition, the UET card software may also include a scheduler **411**, and other utilities, as desired.

The UET Card software also includes modules for I/O drivers **421**, display drivers **422**, utility & command management **423**, clock and calendar **418**, initialization **419**, and authorization/security and signature management **420**.

Initially, when the on/off switch is turned on, the I/O driver detects it and turns on the display and prepares the UET card for use. Thereafter the main display provides options to be selected by the card user through a touch screen. A variety of options are available and UET card can be programmed for special applications as desired. All the individual software blocks outlined here are standard and familiar to any one knowledgeable in the software field.

FIG. **5** shows the CIU hardware **51**. The CIU is used for interconnecting UET Card to PC/POS and the main central computer through normal telephone lines. As shown in FIG. **5**, the CIU includes a display for text **52** which may be a liquid crystal display a cathode ray tube, or some other form of display. It also includes a key pad **53** for dialing and start/stop and special functions, a physical connector **58** to communicate with the UET Card **54**, a telephone line interface **55**, a PC/POS interface **56**, and a power line connector **57**.

FIG. **6** is the block diagram of the CIU. The CIU comprises a microprocessor **61**, a display **62**, which may be a liquid crystal display or other suitable display, keys **63**, a telephone interface **64**, a PC/POS interface **65**, a UET card position **66**, and a UET Card contact **67**.

The software for the CIU is shown in FIG. **7**. It includes I/O drivers **71**, display drivers **72**, utility/command management software **73**, and a POS database **74** to include one or more POS ID numbers, credit card company numbers, service numbers, and department identifications or sales identifications, or the like. It also includes UET card management software **75**, and may also include other software **76**.

When a user of a UET card wishes to use the UET card for a transaction, the card is connected to the CIU unit. When the metal contacts of the UET card are connected to the corresponding contacts or port of the CIU, the CIU software recognizes the UET card contact and prepares itself to read information from the UET card. It also dials the main computer center for verification and interfaces with POS computer. The CIU unit may include software capable of displaying signatures or other types of verification/identification such as photographs, finger prints or voice prints.

The other software **76** for the CIU unit may include an interface for a point of sales computer or for a home computer. It may also include special features, transaction handling, a timer/scheduler, and memory management software.

FIG. **8** illustrates three different versions of the CIU. CIU A is a passive interface between the UET card and a personal computer. CIU A includes metal contacts for connecting with the UET card and a serial port or a parallel port or other

A method for use in the detection of fake mass-produced articles that may be apparently identical to genuine articles involves marking genuine articles with a unique or restricted code mark generated by a secret algorithm, the gamut of such marks being underutilized so that attempts to generate seemingly genuine marks without knowledge of the algorithm will stand only a small chance of success. The marks can be scrutinized for genuineness--whether or not they conform to the algorithm--by a programmable hand held calculator or by a computer. Since one way to produce a seemingly genuine mark would be to copy genuine marks, the calculator or computer is also programmed to detect whether any particular mark has been read before.

7 Claims, 3 Drawing figures

FIG. 20 illustrates a medical "card" as it would be used on the UET card of the present invention.

FIG. 21 illustrates an ID "card" as it would be used on the UET card of the present invention.

FIG. 22 illustrates a phone "card" as it would be used on the UET card of the present invention.

FIG. 23 illustrates an airline "card" as it would be used on the UET card of the present invention.

FIG. 24 illustrates a car rental "card" as it would be used on the UET card of the present invention.

FIG. 25 illustrates special interfaces with the communications interface unit that may be used to handle different protocols used by different service institutions.

FIG. 26 illustrates the use of an alphanumeric keyboard on the touch sensitive display of the UET card.

FIG. 27 illustrates additional features that may be added to the UET card of the present invention.

FIG. 28 outlines a "to do" list on the UET card of the present invention.

FIG. 29 outlines the initialization process for a UET card of the present invention.

FIG. 30 illustrates a variety of interfaces for the UET card of the present invention.

FIG. 31 illustrates a block diagram of a health care service provider system using the UET card of the present invention.

DETAILED DESCRIPTION

The embodiment of the Universal Electronic Transaction (UET) Card shown in FIG. 1 consists of a large full scale liquid crystal display with touch-memory screen **10**, a LED light emitting diode to indicate on/off status **11**, an on/off switch **12**, metal contacts **13** to read/write to and from the memory and to charge the battery through an external unit, such as a communications interface unit, a slide type control to manage display brightness **11**, plastic cover and enclosure **15**, speaker or beeper **16** to activate an audible alarm during low battery or a reminder signal and associated electronics hardware and software to store and analyze personal, account, credit, and transactional information. The size of the UET Card may be around 3½"×2½", which is similar to the normal plastic credit card in use today. It is designed to be carried in the wallet and/or packets.

In the preferred embodiment discussed herein, the user may enter information into the memory of the UET card by touching selected parts of the touch-sensitive display. Alternatively, if the display is not touch-sensitive, the user may input information by using a mouse or other pointing device, which may be in the form of a trackball built into the UET card.

FIG. 2 shows an embodiment of the overall UET card system configuration. It includes a communication interface unit ("CIU") **21**, which interfaces with the UET card either through physical metallic contact—preferred for the touch memory devices—or infra red or radio frequency based wireless transmit and receive units. The CIU includes means for receiving data from the UET card, such as metal contacts to connect to the metal contacts **13** of the UET card, or infrared or radio frequency based wireless systems, depending on the system used by the UET card. In addition, the CIU is provided with memory means for storing data, such as random access memory devices (RAM), means for processing data, such as a microprocessor, and means for directly communicating with the point of sales ("POS") and home or office personal computer ("PC"), such as serial or parallel ports. The CIU is provided with a modem or other suitable means for telecommunicating with remote computers and data base facilities for credit verification, card issuing, bill payments, etc. Some of the features offered by the CIU can also be incorporated directly into UET Card provided the size of the card can remain small enough to carry it in the pockets.

The POS computer **23** interfaces directly with the CIU to read/write information to and from the UET card and communicate with the main central computer of the credit card or bank card company for customer data base, credit verification, etc. The POS computer also writes transaction information directly into the UET Card thereby eliminating need for paper receipts. The POS computer may vary in size, shape and applications, and as a result, the CIU is provided with software which will adapt to a variety of POS computers in use today or which may be used in the future. Software for communicating between computers is readily available in the marketplace today. Alternatively, special software may be written to enable the CIU to communicate with the POS computer.

The home PC **24** interfaces with the UET card to perform transactional analysis needed for tax review, summary, or budgeting purposes. Software for interfacing between the home PC and the UET Card for reading information from the card is available, so long as conventional memory components are used, or can be specially written. Software enabling the PC to dialing directly to the main central computer used by a service institution with whom the user of the UET card has an account is readily available. For the purpose of electronic communications with the service institution, the PC must be equipped with a modem.

At the main central computer a special interface **25** is required with appropriate hardware to concentrate multiple telephone lines, and software to keep the existing methodology and formats used by the credit card and banking industries. The interface also provides caller identification feature normally available from the local telephone companies to add security. Through the caller identification feature, it is possible to identify the location of the originating call for every transaction, such that along with each transaction a telephone number can be tagged to trace misuse of the UET Card. This interface **25** is very similar to the existing interfaces except for the unique software and the added caller identification feature.

The main central computer **26** is used by all the credit card issuing companies or other service providers for management and monitoring. The computer includes customer data base **27**, operator positions **28** for customer services, and facilities to store and process transactions, reports, analysis, account authorization, card issuance and cancellation, etc.

The UET card may be configured with sufficient memory to store all transactions electronically, so as to eliminate or reduce the need for paper receipts. The transactions thus stored in the UET card may be downloaded into another computer, such as the user's home personal computer, or the main computer. The main computer may also be provided with the capability of analyzing transactions, generating reports and issuing new cards electronically by transmitting an electronic image of the card after caller identification and verification. This electronic image may include the name, credit card number, date of issue, date of expiration, credit limits, and a graphic image of the card, along with a variety of coded security information unique to the credit card issuing company and the card holder to eliminate fraud and misuse.

Document Number 2

Entry 4 of 5 File: USPT Sep 5, 1989

US-PAT-NO: 4864110
DOCUMENT-IDENTIFIER: US 4864110 A

TITLE: Electronic payment process using a smart card
DATE-ISSUED: September 5, 1989

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Guillou; Claude L.	Bourgbarre	N/A	N/A	FRX

ASSIGNEE INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Etat Francis/Telediffusion De France	Paris	N/A	N/A	FRX	03

APPL-NO: 7/ 214729
DATE FILED: June 1, 1988
FOREIGN-APPL-PRIORITY-DATA:
FOREIGN-PRIORITY:
FOREIGN-PRIORITY-APPL-NO: FR 86 14378
FOREIGN-PRIORITY-APPL-DATE: October 16, 1986

PCT-DATA:
PCT-DATE-FILED: October 13, 1987
PCT-APPL-NO: PCT/FR87/00397
PCT-371-DATE: June 1, 1988
PCT-102(E)-DATE: June 1, 1988
PCT-PUB-NO: WO88/02900
PCT-PUB-DATE: April 21, 1988

INT-CL: [4] G06K 5/00
US-CL-ISSUED: 235/380; 235/379
US-CL-CURRENT: 235/380; 235/379
FIELD-OF-SEARCH: 235/379, 235/380

REF-CITED:

U.S. PATENT DOCUMENTS

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
4810862	March 1989	Nakano	235/380

FOREIGN PATENT DOCUMENTS

card; selecting at least one service institution account; selecting from the at least one service institution account credit transactions for such account which were transacted in a predetermined period of time; and, transmitting from the universal electronic transaction card the selected credit transactions to storage means in a personal computer. The selected credit transactions may thereafter be displayed on the personal computer in the form of a monthly statement of the type normally provided on paper by the service institution.

The invention also includes a method of using a UET card as a remote terminal for a service institution system. The method includes the steps of selecting a previously authorized service institution account from the universal electronic transaction card; establishing an electronic communication between a personal computer and the service institution system for such service institution account; transmitting to the service institution system from the universal electronic transaction card identifying information for the user and for the service institution account; comparing the identifying information with authorization information in the service institution account to determine if the identifying information is valid; and, for valid identifying information, communicating selected account and transaction information between the universal electronic transaction card and the service information system, responsive to commands communicated from the universal electronic transaction card to the service information system. The selected transactional information may thereafter displayed on the universal electronic transaction card in the form of a monthly statement of the type normally provided on paper by the service institution.

There are several advantages to the present invention. With respect to credit card transactions, the UET card of the present invention may be used to store in memory each credit card or bank transaction for which it is used. Those transactions may be displayed on the display of the UET card. Alternatively, the contents of memory may be electronically transferred to a personal computer for use in any one of a number of commercially available personal accounting programs, such as the program commercially sold under the name "QUICKEN". Alternatively, the information could be used with spreadsheet programs, such as LOTUS or EXCEL. Alternatively, the UET card may be provided with a disk containing a program that may be used on a personal computer to display and print the information. Or, for those card users who might not own a personal computer, a printer may be provided to interface with the card and to print the record of the desired transaction or transactions.

Given the capability of retaining an electronic record of transactions, the user of the UET card would have no need for a paper record of the transaction, and the paper receipt at the point of sale could be eliminated. Further, since the information concerning each credit card transaction would be recorded in the memory of the UET card at the time of the transaction, there would be no need for the generation of a monthly statement from the credit card provider to the UET card owner. In fact, the UET card owner could eliminate all paper transactions and bills by using an electronic method of paying the credit card provider by any one of the methods that are currently available.

There are also several advantages that may be realized by the application of the present invention to the health care industry. A patient's insurance information, and key medical history information may be maintained in the memory of the UET card. Alternatively, or in addition, a patient's complete medical history may be maintained in a universal database, accessible over a health care data network similar to the network presently known as the INTERNET. Thus, every time a patient using a UET card would visit a doctor, or a hospital, or an out patient clinic, or a pharmacy, the patient's medical history would be available so that the health care provider or pharmacist would have instant access to information that might prevent the prescribing of drugs or other treatment which would not be tolerated by the patient, because of allergic reactions or other contraindications.

The foregoing advantages are some examples of the advantages provided by the present invention, and are not intended to be exhaustive. Specific examples of the implementation of the invention are shown in the drawings and are discussed herein. Those examples are intended provide examples of the invention, not to limit it. The scope of the invention is expressed in the claims.

DESCRIPTION OF THE DRAWINGS

FIG. **1** is a front view of one embodiment of a universal electronic transaction card in accordance with the present invention.

FIG. **2** is a block diagram illustrating one embodiment of a universal electronic transaction card system in accordance with the present invention.

FIG. **3** is a block diagram of one embodiment of the UET card of the present invention.

FIG. **4** is a functional diagram of the software blocks used in one embodiment of the UET card.

FIG. **5** is a front view of one embodiment of a communication interface unit of the present invention.

FIG. **6** is a block diagram of one of the components of the communication interface unit of the present invention.

FIG. **7** is a block diagram of the software blocks used in one embodiment of the communication interface unit of the present invention.

FIG. **8** is a diagram illustrating three different versions of a communication interface unit used in the present invention.

FIG. **9** illustrates one embodiment of the display of the UET card of the present invention.

FIG. **10** illustrates a signature made by a user on the display of the UET card of the present invention.

FIG. **11** illustrates a manner of inputting a security code on the UET card of the present invention.

FIG. **12** illustrates a menu for selecting from groups of service institution transactions.

FIG. **13** illustrates a menu for selecting from credit card transactions after selection of credit from the menu shown in FIG. **12**.

FIG. **14** illustrates a menu for user commands for a credit card transaction for the UET card of the present invention.

FIG. **15** illustrates a status display on the UET card of the present invention during a transaction.

FIG. **16** illustrates another status display on the UET card of the present invention during a transaction.

FIG. **17** illustrates a status display upon completion of a transaction.

FIG. **18** illustrates commands that may be used on the UET card of the present invention.

FIG. **19** illustrates an ATM bank "card" as it would be used on the UET card of the present invention.

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY
904689	August 1986	BE
0227532	July 1987	EP
2403597	April 1979	FR
2503423	October 1982	FR
6077993	October 1978	CH

ART-UNIT: 235
PRIMARY-EXAMINER: Pitts; Harold I.
ATTY-AGENT-FIRM: Oblon, Spivak, McClelland, Maier & Neustadt

ABSTRACT:

The storage cells are grouped into elements grouping at least two cells, each element being locatable by an address and having a parity. The balance of the card is the number of non-zero even elements with an address below the address of the odd element with the lowest address and which is called the "terminal". In order to debit the card and reduce said balance, the terminal is moved towards a lower address, while creating a new old element of lower address than the terminal to be displaced. In order to credit the card and increase this balance, the terminal is moved towards a higher address, while again giving to possible odd elements with a higher address than the terminal to be displaced an even character and while creating a new odd element with a higher address than the terminal to be displaced.

5 Claims, 11 Drawing figures

device to the personal computer, where it may be processed by the computer to produce electronic reports in the nature of monthly statements now received from service institutions. In addition, modem communications with a central system may be done by the personal computer. Alternatively, in the UET card and communications system, the CIU device may comprise a passive interface with the universal electronics transactions card and a modem. Or, the CIU may have more features, including a passive interface with the universal electronics transactions card, a modem, means for processing information, means for storing information, input means for entering information, and display means for displaying information.

The invention also includes an electronic transaction system which includes a plurality of UET cards, CIU devices, point of transactions systems, and an institutional system. The point of transactions system includes means for inputting and storing transactional information; means for electronically communicating with the UET card to receive account information; means for electronically communicating the account information and transactional information to an institutional system; and means for electronically communicating transactional information to the personal electronic transaction card. The communications between the UET card and the point of transactions system may be done through the CIU device. The institutional system includes means for creating account numbers; means for assigning and authorizing account numbers; means for electronically communicating an authorized account number to a universal electronic transaction card; means for receiving and storing personal information for each authorized account number; means for communicating with a personal electronic transaction card to authorize account transactions, and means for receiving and storing information relating to account transactions. Communications systems are provided to enable communications between the universal electronic transaction card and point of transactions system and between the point of transactions system and the institutional system, including card interfacing means for interfacing between the transactional provider system and the universal electronic transaction card to exchange electronic information; and communications means for communicating with the institutional system.

In one application of this invention, a health care management system is provided in which UET cards are used for inputting, storing, processing, and transmitting personal information, including personal medical history, account information, and transactional information. At least one central health care information processing system is provided, and it includes means for creating, assigning and storing patient and health care provider accounts; means for electronically communicating account information to a universal electronic transaction card; means for receiving and storing personal information for each authorized account number; means for communicating with a universal electronic transaction card to authorize account transactions, means for receiving and storing information relating to account transactions; and means for storing and communicating medical histories. In this system, the UET card is used by a patient when the patient visits the health care provider. Health care providers may include doctors, hospitals, laboratories, pharmacies, out patient clinics, and the like. Health care providers use a health care provider processing system, which includes means for electronically communicating with the central health care information processing system; means for electronically communicating with the UET card; and memory means for storing patient information. Communications systems are also provided for providing communications between the universal electronic transaction card, the central health care information processing system, and the health care provider processing system.

When a patient visits a health care provider, the patient's UET card is interfaced with the health care provider processing system, which in turn may communicate with the central health care processing system. All pertinent information concerning the patient's health is then instantly available to the health care provider, including the patient's medical history, insurance coverage, and the like. After the patient is treated, or is provided with a medical service, billing is automatically done by the system, and all pertinent information concerning the billing is electronically transmitted to the patient's UET card and also to the appropriate service institution.

This invention also includes a method of conducting an electronic credit transaction using a service institution account which includes the steps of (1) selecting from a UET card a service institution account from a group of service institution accounts; (2) establishing an electronic communication between the universal electronic transaction card, a point of transaction system and a service institution system; (3) transmitting from the universal electronic transactions card to the point of transaction system the account information for the selected service institution account; (4) transmitting from the point transaction system to the service institution system transactional information for the credit transaction and the service institution account; (5) in the service institution system, screening the service account and transactional information to determine whether the account is valid and whether the credit transaction is within predetermined credit limits for that account; and (6) for valid accounts and credit transactions within predetermined limits, transmitting an authorization for the credit transaction to the point of transaction system, storing the transactional information for the credit transaction in the service institution system with respect to the service institution account, and transmitting the transactional information for the credit transaction to the universal electronic transaction card and storing the transactional information for the credit transaction in the universal electronic transaction card with respect to the service institution account.

This invention also includes a method of issuing an account by a service institution to a user of a universal electronic transaction card to authorize the user to use the universal electronic transaction card for the account. The method includes the steps of (1) obtaining predetermined information from the user as required by the service institution; (2) issuing account information for the user, including an account number; and (3) electronically transmitting to the user's universal electronic transaction card predetermined account information for the service institution account and predetermined information about the service institution and the account to be displayed by the universal electronic transaction card when the universal electronic transaction card is used to conduct a credit transaction for such account. Among other things, the predetermined information may include the name of the service institution account service and a graphic image of the service institution's account service logo.

This invention also includes a method of transferring account information and accumulated transactional information for a plurality of credit transactions for a service institution account from a UET card to a personal computer. The method comprises the steps of establishing an electronic communication between a personal computer and a UET

Document Number 3

Entry 3 of 5 File: USPT Feb 19, 1991

US-PAT-NO: 4995082
DOCUMENT-IDENTIFIER: US 4995082 A

TITLE: Method for identifying subscribers and for generating and verifying electronic signatures in a data exchange system
DATE-ISSUED: February 19, 1991

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Schnorr; Claus P.	6350 Bad Nauheim	N/A	N/A	DEX

APPL-NO: 7/ 484127
DATE FILED: February 23, 1990
FOREIGN-APPL-PRIORITY-DATA:
FOREIGN-PRIORITY:
FOREIGN-PRIORITY-APPL-NO: EP 89103290.6
FOREIGN-PRIORITY-APPL-DATE: February 24, 1989

INT-CL: [5] H04K 1/00
US-CL-ISSUED: 380/23; 380/30, 380/25, 380/46
US-CL-CURRENT: 713/169; 380/30, 380/46, 705/67, 713/180
FIELD-OF-SEARCH: 380/28, 380/30, 380/25, 380/46, 380/23

REF-CITED:

U.S. PATENT DOCUMENTS

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
4225935	September 1980	Zscheile et al.	380/28
4351982	September 1982	Miller et al.	380/30
4405828	September 1983	Rivest et al.	380/30
4514592	April 1985	Miyaguchi	380/28
4658094	April 1987	Clark	380/30
4748668	May 1988	Shamir et al.	380/28
4759063	July 1988	Chaum	380/28
4759064	July 1988	Chaum	380/28
4876716	October 1989	Okamoto	380/30

OTHER PUBLICATIONS

Omura, J. K., "A Computer Dial Access System Based on Public-Key Techniques", I.E.E.E., Communcations, vol. 25, No. 7, 1987, pp. 73-79.
Beth, T., "Efficient Zero-Knowledge Identification Scheme for Smart Cards", Advances in Cryptology-Eurocrypt, '80, pp. 77-84.

ART-UNIT: 222
PRIMARY-EXAMINER: Tarcza; Thomas H.
ASSISTANT-EXAMINER: Cain; David
ATTY-AGENT-FIRM: Hill, Van Santen, Steadman & Simpson

computers, including those used by retailers (point of sale computers), and personal computers used in other business applications or at home.

In one embodiment of the invention, a UET card is provided for storing, transmitting, and receiving information for a plurality of service institutions. As used herein, the term "service institution" includes any business, service, governmental agency, or other entity, which issues any type of card commonly carried by an individual for the purposes of identification, credit transactions, bank transactions, licensing, registration or similar functions. The information stored, transmitted, or received by the UET card may include personal information of the user of the UET card. It may also include account information for each service institution with which the user has an account. As used herein, the term "account information" includes any identifying designation which identifies the UET card user with a service institution, including but not limited to the user's name, address, phone number, social security number, credit card account numbers, bank account numbers, license numbers, identification numbers, insurance account numbers, medical identification numbers, and the like. The information stored, transmitted, or received by the UET card may also include transactional information for accounts with service institutions in which the UET card user has an account. As used herein, the term "transactional information" includes information relating to one or more individual financial transactions, such as credit card transactions, medical treatment payments, insurance payments, and the like. The transactional information includes various transaction details that may appear on a paper receipt for any given financial transaction, such as a subtotal, a tip, if any, a transaction total, the date and place of the transaction, and the user's signature.

The UET card comprises housing means adapted to fit in a pocket or a purse which houses inputting means, memory means, communications means, display means, and processing means. Inputting means are provided for inputting information, including personal information for the user, account information for a plurality of service institutions in which the user has an account, and transactional information for each service institution for which account information exists. Memory means are provided for storing the information inputted by the inputting means. Communications means are provided for electronically communicating information stored in the UET card. The UET card includes display means for displaying information for a plurality of service institution accounts, including personal information, account information, and transactional information. In a preferred embodiment the display means comprises a touch-sensitive LCD display. In a preferred embodiment, the UET card is also provided with processing means for processing information, although if required by cost considerations, the processing means could be provided by a personal computer or a communications interface unit (which is described below). Means are also provided for providing and storing electric power and for selectively providing power to the components of the UET card. The UET card also includes security means for preventing unauthorized use of the universal electronic transaction card and for preventing unauthorized access to the information stored in the memory means of the universal electronic transaction card.

In a preferred embodiment, the UET card includes a touch-sensitive display which is large enough to display a visibly perceptible replica of a credit card and a visibly perceptible replica of the user's signature. Menus can be provided on the touch sensitive display to enable the user to select one service institution from a group of service institutions in order to proceed with a transaction using the card. Further, the touch-sensitive display may be provided with multiple levels of menus, including at least one level enabling the user to select from groups of service institutions, and at least one other level enabling the user to select a particular service institution. In addition, a graphic image of a service institution may be displayed when the service institution is selected by a user, along with the user's name and account number. Alternatively, instead of a touch-sensitive display, the UET card may be provided with a pointing device.

The UET card can also be provided with a variety of other menus, which permit the user to review account information for a selected service institution, or a record of transactions with a service institution. In addition, the user's signature can be inputted into the UET card and thereafter displayed for security purposes. The electronic transaction card may further include means for automatically cancelling at least one account in the event that a non-authorized user attempts to use the card to conduct an unauthorized transaction with the user's account.

The UET may also include power means for selectively providing power to the display means, the processor means and the communication means. In one such embodiment, the means for providing and storing electric power includes first power means for providing backup power to the memory means and second power means for selectively providing power to the memory means, inputting means, display means, processing means and communications means. In addition, the UET card may further be provided with means for detecting inputting and processing activity and for turning off power to display means and processing means upon detecting no inputting or processing activity for a predetermined time interval.

The present invention also provides for a universal electronic transactions card and communications system ("UET card and communications system") for storing, transmitting, and receiving the type of information discussed above for a plurality of service institutions. The system includes a plurality of UET cards adapted to fit in a pocket or a purse and a plurality of communications interface units ("CIU"). At a minimum, the UET cards must include memory storage devices and means for electronically transmitting information to and from the UET memory. Preferably, the UET cards in this UET card and communication system are also provided with touch-sensitive display means, and processing means. Either the UET card or the CIU device must have display means for displaying information for a plurality of service institution accounts, including personal information, account information, and transactional information; processing means for processing information, including personal information, account information, and transactional information; means for providing and storing electric power and for selectively providing power to the memory means, inputting means, display means, processing means and communications means; and, security means for preventing unauthorized use of the universal electronic transaction card and for preventing unauthorized access to the information stored in the memory means of the universal electronic transaction card.

Thus, in the UET card and communications system, the CIU device may comprise a passive interface between the universal electronics transaction card and a personal computer. In that event, the UET card may be equipped with memory, processing means, touch-sensitive display means, and means for interfacing with the CIU device. Information may be communicated from the UET card through the CIU

ABSTRACT:

In a data exchange system working with processor chip cards, a chip card transmits coded identification data I, v and, proceeding from a random, discrete logarithm r, an exponential value x=2.sup.r (mod p) to the subscriber who, in turn, generates and transmits a random bit sequence e to the chip card. By multiplication of a stored, private key s with the bit sequence e and by addition of the random number r, the chip card calculates a y value and transmits the y value to the subscriber who, in turn, calculates an x value from the information y, v.sub.j and e and checks whether the calculated x value coincides with the transmitted x value. For an electronic signature, a hash value e is first calculated from an x value and from the message m to be signed and a y value is subsequently calculated from the information r, s.sub.j and e. The numbers x and y then yield the electronic signature of the message m.

11 Claims, 5 Drawing figures

UNIVERSAL ELECTRONIC TRANSACTION CARD INCLUDING RECEIPT STORAGE AND SYSTEM AND METHODS OF CONDUCTING ELECTRONIC TRANSACTIONS

BACKGROUND OF THE INVENTION

This invention relates to a universal electronic transaction card ("UET card") for storing, transmitting and receiving personal, accounting and transactional information, to a UET card and communications systems, and to an electronic transaction system which utilizes UET cards. This invention also relates to a health care system utilizing UET cards. This invention also relates to methods of issuing an account authorization to a UET card, a method of transferring transactional and account information between a UET card and a personal computer or a mainframe computer, a method of using the UET card as a remote terminal for a mainframe computer, and a method of conducting an electronic transaction. The UET card of the present invention is capable of functioning as a number of different credit cards or other transaction or identification cards, which provides the user of the UET card with the capability of selecting one of many such cards for use in a particular transaction. The UET card of this invention has universal application for all personal and financial transactions, such as normal credit card usage of the type commonly associated with MASTERCARD, VISA, AMERICAN EXPRESS or automatic banking transactions (known as "ATM" transactions); health service transactions, such as physicians' services, hospital services, or home health care services; personal identification, including social security number, signature, photograph, and other personal information; employee information, such as employee identification numbers; and license information, including drivers licenses, vehicle registrations, professional licenses, and the like.

Presently, plastic cards are used for a variety of transactions, such as credit card purchases, and automatic banking transactions. Such credit cards include a magnetic strip that contains coded information for account information and, in some cases, a security code. The coded information on the magnetic strips is read by a device in the possession of a merchant, which transmits the account information to a central computer, which determines whether the account number is valid and whether the purchase is within the amount of credit available for that account. If the transaction is authorized, the card user receives a paper receipt as his or her record of the transaction, and the retail merchant also keeps a copy of the receipt as a record of the transaction. Later, usually within 30 days, the card user receives a written statement, which, in the case of a credit card, contains an invoice for payment. The user must then write a check to the credit card company to pay the amount due on the account. The disadvantage of the foregoing system is that at least two written documents are generated for the credit card user, at a substantial cost to the credit card institution.

In the case of ATM banking machines, a banking card is inserted into the card reader of the machine, which reads the coded account information and security code. The card user then enters a security code. If the security code is correct, the card user is then able to perform a banking transaction in which he or she may either deposit money, withdraw money, or check account balances. The ATM card user receives a paper receipt for the transaction. Later, the ATM card user also receives a paper record of all of his or her transactions for the month from the banking institution.

Every day, at least tens of millions of credit card and ATM transactions take place. Each transaction gives rise to the creation of several pieces of paper relating to billing for the goods or services purchased by credit card. Elimination of all or a substantial amount of paper associated with those transactions would reduce the costs of providing credit card services and would reduce the amount of waste generated and energy used as a result, and would improve the environment. Further, conversion of the manual billing system could eliminate substantial labor costs and also reduce the amount of human error in credit card transactions.

The same is true of the health care industry. A substantial amount of paper is generated by the health care industry, including insurance cards, medical identification cards, medical bills, medical history reports, and the like. A substantial amount of personal health care information must be manually entered for each visit by a patient to a health care provider. Each visit usually results in filling out one or more insurance forms that are, in turn, sent to insurance companies for processing. Approximately 15% of the cost of health care is spent on insurance companies who process payments and claims. The substantial reduction or elimination of paper work associated with health care, and the conversion to a paperless billing system could greatly reduce the labor costs associated with health care, and thereby reduce health care expenses considerably.

Most people carry a substantial number of cards, including multiple credit cards, insurance cards, drivers' licenses, airline cards, check identification cards, ATM cards, and employee identification cards. Carrying a substantial number of such cards is inconvenient. Financial accounting associated with these cards related to paying bills, keeping track of accounts, budgeting, planning and the like, is manual, cumbersome, time consuming, and difficult to manage and maintain. Further, such cards are replaced on a periodic basis. Thus, a substantial amount of plastic must be used to make the cards, paper must be used to mail the cards to users, and a substantial amount of paper and plastic is eventually thrown away, resulting in waste, degradation of the environment, and a loss of money.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a universal electronic transaction card ("UET card") which is capable of storing, transmitting and receiving personal and transactional information and thereby replacing plastic cards, which are presently used for the same purpose. In one form of the invention, the universal electronic transaction card of the present invention is a pocket sized device, which includes a microprocessor, random access memory, a display, and input means, and is capable of storing personal information such as the card owner's name, address, date of birth, signature, and likeness, as well as the user's social security number. The UET card is also capable of storing the user's employee number (if applicable), insurance policy number or numbers for various type of insurance, club membership account numbers, credit card company account numbers for a variety of credit card companies, automatic banking numbers for one or more bank accounts, and any other financial or personal transactional information. The UET card is also capable of processing transactional information and communicating with central processing units or computers operated by the providers of services, such as credit card institutions, banks, health care providers, retailers, wholesalers or other providers of goods or services. The UET card is also capable of communicating with personal

Document Number 4

Entry 2 of 5 File: USPT Aug 18, 1992

US-PAT-NO: 5140634
DOCUMENT-IDENTIFIER: US 5140634 A

TITLE: Method and apparatus for authenticating accreditations and for authenticating and signing messages
DATE-ISSUED: August 18, 1992

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Guillou; Louis C.	Rennes	N/A	N/A	FRX
Quisquater; Jean-Jacques	Brussels	N/A	N/A	BEX

ASSIGNEE INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
U.S Philips Corporation	New York	NY	N/A	N/A	02

APPL-NO: 7/ 776701
DATE FILED: October 9, 1991
PARENT-CASE:
This is a continuation of application Ser. No. 07/704,891, filed on Feb. 22, 1990 which is a continuation of Ser. No. 07/241,527, filed on Sep. 7, 1988, both abandoned.
FOREIGN-APPL-PRIORITY-DATA:
FOREIGN-PRIORITY:
FOREIGN-PRIORITY-APPL-NO: FR 87 12366
FOREIGN-PRIORITY-APPL-DATE: September 7, 1987

INT-CL: [5] H04K 1/00, H04K 9/00
US-CL-ISSUED: 380/23; 380/24, 380/25, 380/30, 235/382
US-CL-CURRENT: 713/180; 235/382, 380/30, 705/67, 713/172
FIELD-OF-SEARCH: 380/23, 380/24, 380/25, 380/30, 235/382

REF-CITED:

U.S. PATENT DOCUMENTS

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
4200770	April 1980	Hellman et al.	N/A
4295039	October 1981	Stuckert	N/A
4351982	September 1982	Miller et al.	N/A
4638120	January 1987	Herve	N/A
4736423	April 1988	Matyas	380/23
4799258	January 1989	Davies	380/21
4811393	March 1989	Hazard	380/21

ART-UNIT: 222
PRIMARY-EXAMINER: Buczinski; Stephen C.
ATTY-AGENT-FIRM: Barschall; Anne E.

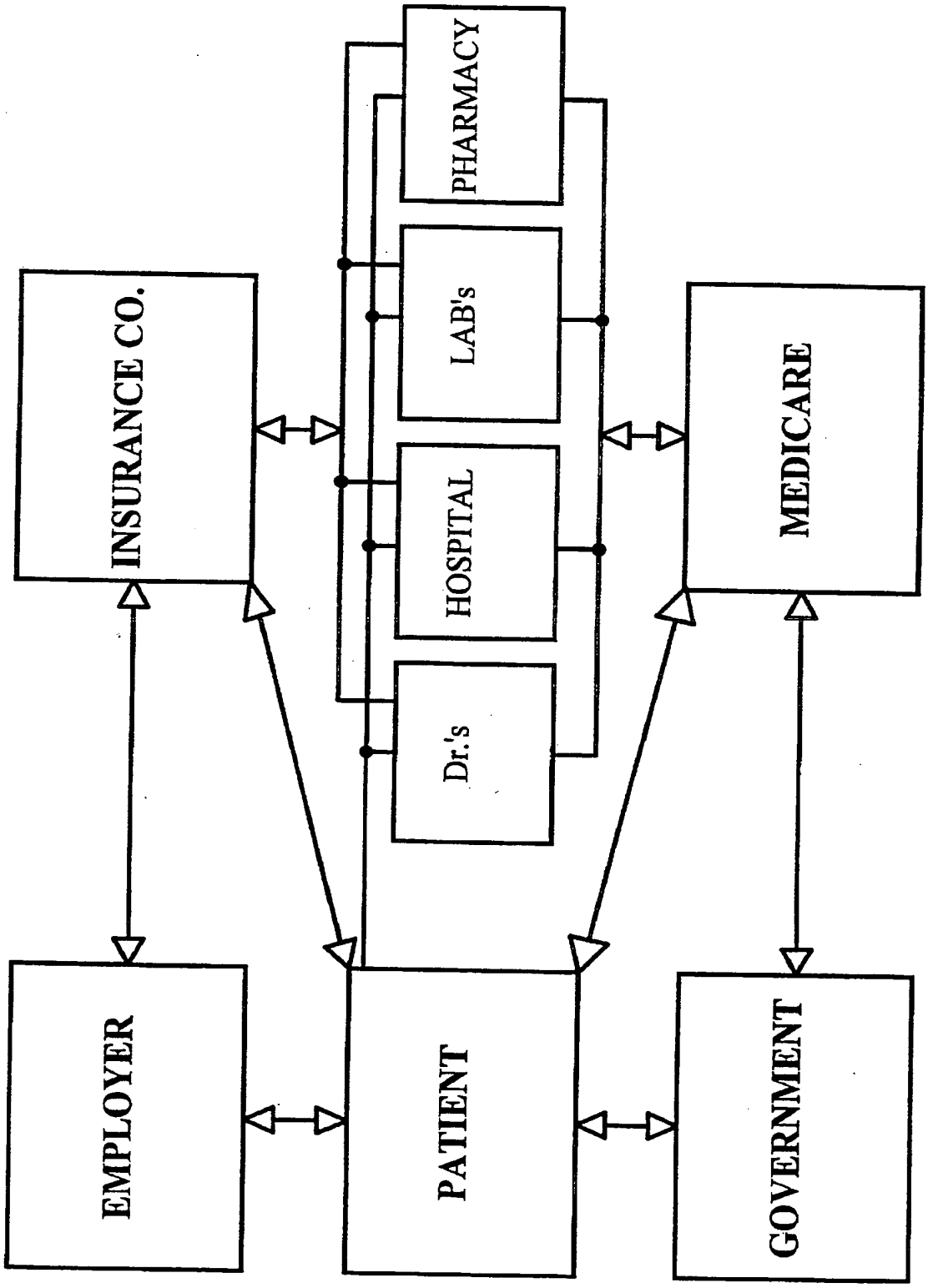
PHARMACY
LAB's
HOSPITAL
Dr.'s
INSURANCE CO.
MEDICARE
EMPLOYER
PATIENT
GOVERNMENT

FIG. 31

ABSTRACT:

A method and system for authentication of accreditations and of messages with zero-knowledge proof and for the signing of messages, and a station for use in such system, in particular executed as a smart card station.

Instead of using multiple accreditations and an iterative process of verification, use is made of a comprehensve accreditation (high exponent p) and a number D is drawn at random, which number is within the range between 0 and p-1. The operations of verifiction proceed by the computation of the D-th power of the inverse accreditation B.

Application in particular, to smart cards and, more specifically, to bank cards.

23 Claims, 10 Drawing figures

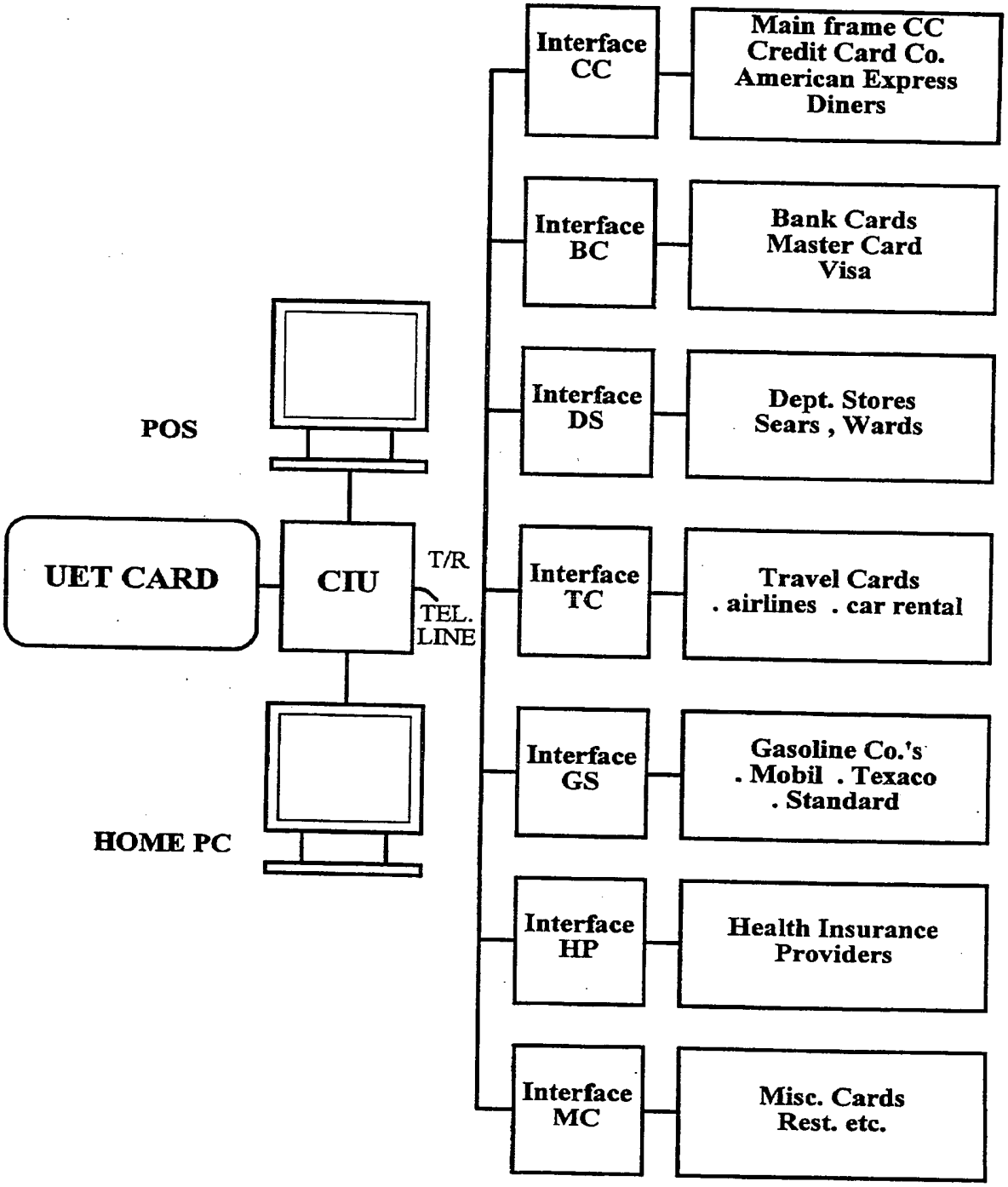
Interface CC
Main frame CC
Credit Card Co.
American Express
Diners
Interface BC
Bank Cards
Master Card
Visa
Interface DS
Dept. Stores
Sears , Wards
POS
UET CARD
CIU
T/R
TEL. LINE
Interface TC
Travel Cards
. airlines . car rental
Interface GS
Gasoline Co.'s
. Mobil . Texaco
. Standard
HOME PC
Interface HP
Health Insurance
Providers
Interface MC
Misc. Cards
Rest. etc.

FIG. 30

WEST

Help Logout

Main Menu | Search Form | Result Set | Show S Numbers | Edit S Numbers | Referring Patents

First Hit | Previous Document | Next Document

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC

Document Number 5

Entry 1 of 5 File: USPT Nov 22, 1994

US-PAT-NO: 5367148
DOCUMENT-IDENTIFIER: US 5367148 A

TITLE: Counterfeit detection using ID numbers with at least one random portion

DATE-ISSUED: November 22, 1994

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Storch; Leonard	New York	NY	N/A	N/A
Van Haagen; Ernst	New York	NY	N/A	N/A

ASSIGNEE INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Cias, Inc.	New York	NY	N/A	N/A	02

APPL-NO: 7/ 669904
DATE FILED: March 15, 1991

PARENT-CASE:
This application is a continuation in part of copending application Ser. No. 07/420,101, filed Oct. 11, 1989,titled "OPTIMAL, ERROR-DETECTING, ERROR-CORRECTING AND OTHER CODING AND PROCESSING, PARTICULARLY FOR BAR CODES, AND APPLICATIONS THEREFOR SUCH AS COUNTERFEIT DETECTION," and this application is a continuation in part of copending application Ser. No. 292,569, filed Dec. 30, 1988, titled "INFORMATION TRANSFER AND USE, PARTICULARLY WITH RESPECT TO COUNTERFEIT DETECTION," which is a continuation of application Ser. No. 853,745, filed Apr. 18, 1986, now U.S. Pat. No. 4,814,589, titled "INFORMATION TRANSFER AND USE, PARTICULARLY WITH RESPECT TO OBJECTS SUCH AS GAMBLING CHIPS," the disclosures of all of which are incorporated herein by reference.

INT-CL: [5] G06F 15/21

US-CL-ISSUED: 235/375; 283/901, 340/825.34
US-CL-CURRENT: 235/375; 283/901, 340/825.34

FIELD-OF-SEARCH: 340/825.34, 235/375, 235/385, 283/901, 283/903, 283/904

REF-CITED:

U.S. PATENT DOCUMENTS

INITIALIZATION PROCESS

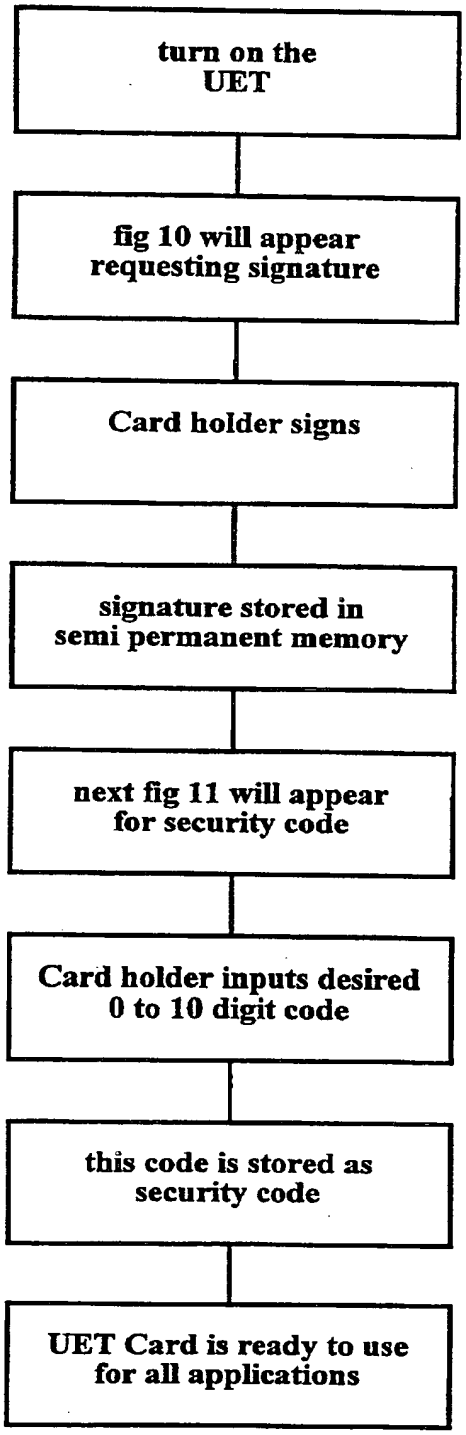

FIG. 29

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
3034643	May 1962	Keller et al.	N/A
3426879	February 1969	Walker	N/A
3524163	August 1970	Weiss	N/A
3829661	August 1974	Silverman et al.	N/A
3833795	September 1993	Shoshani et al.	101/72
3890599	June 1975	Simjian	340/825.34
4087092	May 1978	Krause et al.	N/A
4139219	February 1979	Herndon	283/57
4157829	June 1979	Goldman et al.	N/A
4191376	March 1980	Goldman et al.	235/385
4193061	March 1980	Zoltai	340/825.34
4207814	June 1980	Schenk	235/437
4283709	August 1981	Lucero et al.	235/375
4463250	July 1984	McNeight et al.	235/385
4480177	October 1984	Allen	235/379
4506914	March 1985	Gobeli	283/70
4514815	April 1985	Anderson	364/478
4558318	December 1985	Katz et al.	235/375
4605846	August 1986	Duret et al.	235/468
4630201	December 1986	White	364/408
4641017	February 1987	Lopata	235/457
4677604	June 1987	Selby, III et al.	369/33
4837425	June 1989	Edwards	235/457
4983817	January 1991	Dolash et al.	235/462

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY
10496	April 1980	EP
2237911	March 1973	DE

OTHER PUBLICATIONS

"Appendix C" and paragraph 2.4 of the Invitation for Bid for Optical Bar Code Readers of the Massachusetts State Lottery Commission, dated Apr. 4, 1989.

ART-UNIT: 254

PRIMARY-EXAMINER: Shepperd; John

ATTY-AGENT-FIRM: Rosen, Dainow & Jacobs

ABSTRACT:

Counterfeit objects, such as products or documents, can be detected by checking associated ID numbers, which include one or more appended fields of one or more randomly selected digits, in a database containing the correct authorized ID numbers. This use of random selection makes it impossible for counterfeiters to effectively predict or anticipate correct ID numbers. For example, by using bar coded ID numbers with two distinct appended fields of randomly selected numbers, instead of traditional serial numbers, counterfeit products can be conveniently and positively detected either on a wholesaler's or vendor's shelf using a truncated outside ID number found on the product's packaging, or, for example, upon receipt of a customer's product registration card on which the complete inside ID number is found, this complete inside ID number having been concealed from casual perusal during the product's distribution. If authorized ID numbers are repeated by counterfeiters, "hot" lists are formed and used for immediate detection of counterfeit.

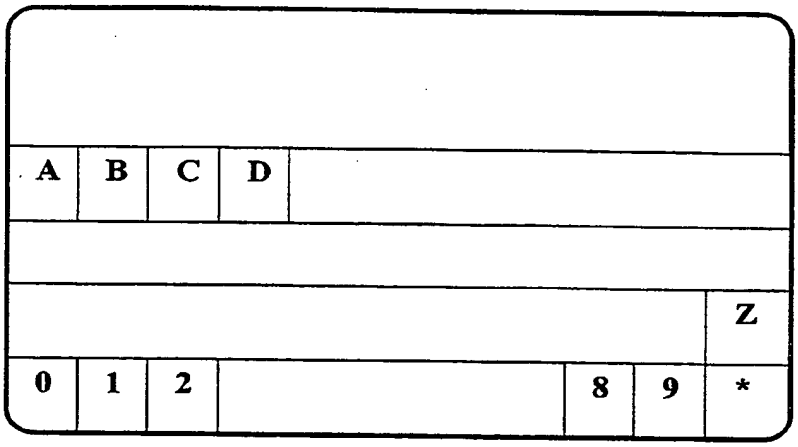

FIG. 26

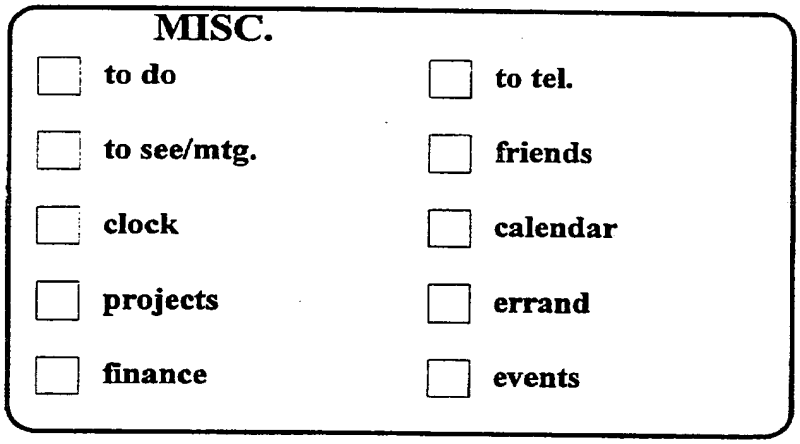

FIG. 27

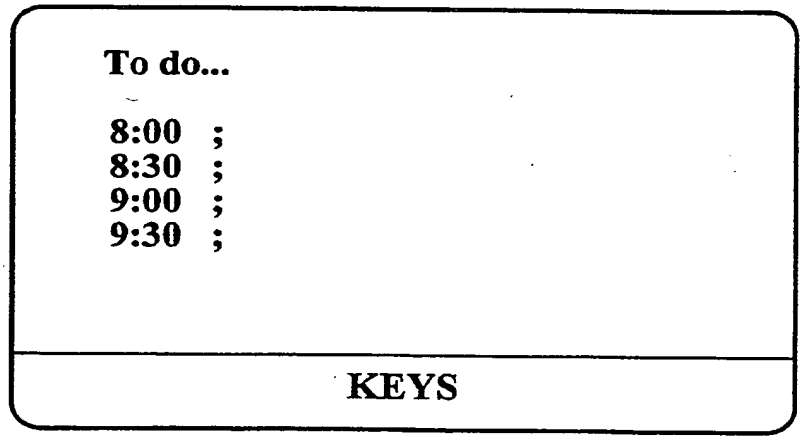

FIG. 28

11 Claims, 4 Drawing figures
Exemplary Claim Number: 1,9,11
Number of Drawing Sheets: 3

BRIEF SUMMARY:

BACKGROUND OF THE INVENTION

The invention disclosed herein relates to counterfeit detection methods.

When an object, such as a product or document, is worth disproportionately more than the cost of its manufacture, it may be counterfeited at a profit. For example, manufacturers of proprietary products lose billions of dollars each year because their most successful products are often targeted by counterfeiters who produce spurious goods locally or overseas. When counterfeit goods are of similar or identical quality to the original, a manufacturer suffers from a continuous loss of sales as counterfeiting continues unchecked, because detection is difficult or impossible. Inferior counterfeit products may be more easily detected, but in addition to the above, they also jeopardize future sales of non-counterfeited products by marring reputation. In either case, the manufacturer's continuing level of untold lost profits due to counterfeit may be dramatic. Similar concerns arise with counterfeit documents.

A partial listing of products susceptible to being counterfeited includes: airplane parts; art; auto parts; baby products--formula, diapers, clothing; books; computers; computer peripherals; cosmetics; designer goods--clothing, shoes, eye glasses; electronics; entertainment recordings--CDs, records, audio and video cassettes; games-board, firmware, handheld; military parts; optics--binoculars, cameras; pharmaceuticals; software; tools; toys; watches.

Documents susceptible to fraud (including counterfeit) include: betting tickets (lottery, sports, etc); bonds (Treasury, commercial, etc); certificates (birth, gift, warranty, etc); checks (personal, commercial, travelers, etc); coupons; credit cards; currency; licenses (driver, business, import/export, etc); passports; scrip (store, amusement park, etc); stamps (postage, food, etc); stocks; tickets (concerts, sports, theater, etc); travel tickets (airline, commuter, etc), and so forth.

Staggering losses due to counterfeit are estimated. For example, the International Anti-Counterfeiting Coalition, IACC, located in Washington, D.C., fears annual losses of $100,000,000,000 (no mistake--one hundred billion dollars!). On Apr. 23, 1990, U.S. Attorney Stephen J. Markman reported the following to the IACC:

"In addition to safety, the economic loss from

counterfeit products is enormous: The big three automakers estimate that they lose 240,000 jobs each year in the greater Detroit metropolitan area a/one due to counterfeiting of auto parts."

Two approaches for detecting counterfeit are: mechanical-based on conformity, and intellectual--based on uniqueness. These two counterfeit detection philosophies are based on fundamental underlying principles which are diametrically opposed to each other, conformity versus uniqueness.

Mechanical counterfeit detection techniques require physical examination and/or analysis of the object. The underlying principle here is conformity. Genuine objects are identical to each other while counterfeits must somehow be different. The difference between the genuine and fake must be discernible in order to detect counterfeit. For example, all U.S. currency is printed on special paper. Therefore, if a suspected bill's paper is discovered to be different, the bill is counterfeit.

Mechanical means alone cannot be relied upon. What one can make or print, another can as well. This creates inherent weaknesses. For example, some counterfeiters of U.S. currency have outwitted the special paper deterrent scheme described above by bleaching the ink off $1 bills and reusing the paper to print $100 bills, while other counterfeiters manufacture their own

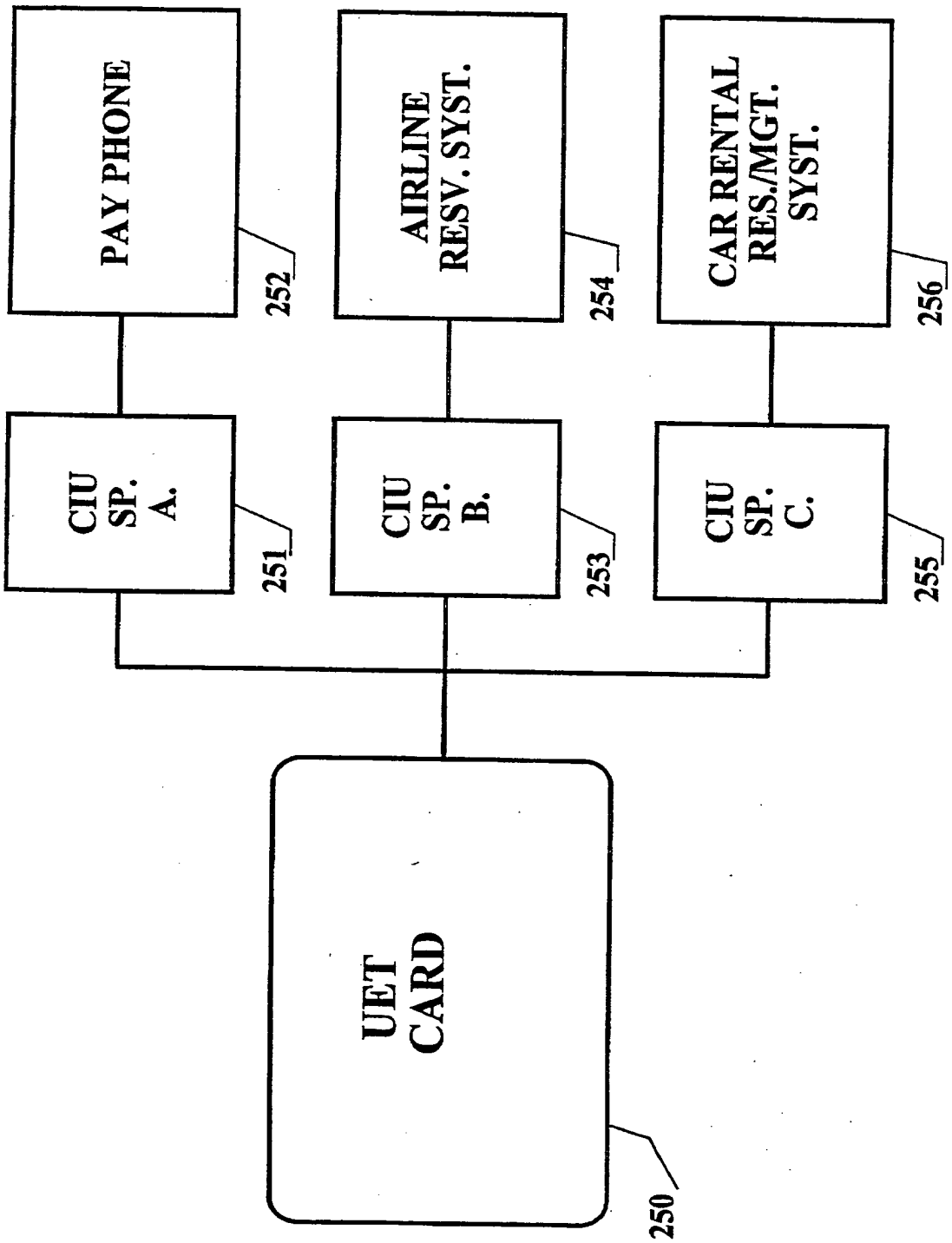
PAY PHONE
252
AIRLINE RESV. SYST.
254
CAR RENTAL RES./MGT. SYST.
256
CIU SP. A.
251
CIU SP. B.
253
CIU SP. C.
255
UET CARD
250

FIG. 25

special paper which is sufficiently similar for their purposes.

Intellectual counterfeit detection and/or authentication techniques may; include signatures, numbers and/or other indicia for coding each genuine object differently. The underlying principle here is uniqueness. Each genuine object is individually signed, or assigned individual identifying information. Traditional ways to individually authenticate objects are: sign or assign.

One traditional way to authenticate certain objects, namely documents, is to sign them. Each person's signature is effectively different. Even though many may be named John Smith or Chun Lee, i.e., many have the same indistinguishable identifying name, respective signatures are different. Typically, fraud involving documents with individuals' signatures thereon is characterized as forgery, versus counterfeit.

For example, valid serial numbers may readily be anticipated and printed by counterfeiters using available numbering devices, while forging a signature is another matter. Blank checks, available at stationery stores, for example, may be authorized by John Smith's signature if he is known, or if that signature is verifiable, perhaps by comparison to other signed documents. Signatures, for example, bridge mechanical and intellectual techniques, involving examination-by-eye.

Applicants' anti-counterfeit techniques address mass produced objects, unsigned products and documents, manufactured to be essentially identical to each other-the only convenient and distinguishable difference among such essentially identical objects being the presence of associated identifying information, such as serial numbers.

Mr. Smith's signed check, mentioned above, may involve other variable information. For example, the dollar amount, the transaction date, payee information, Mr. Smith's address and bank account number, information about his bank, and so forth. Examples of other articles with variable parameters are: birth certificates, credit cards, lottery tickets, passports, etc.

Applicants' address how to detect counterfeit objects among essentially identical objects, objects that do not have individually and/or inherently variable parameters, objects such as mass produced products and documents, objects that may be readily identified only by their respective identifying information.

This is not to suggest that certain aspects of applicants' inventions may not be used beneficially in association with signed documents, for example, to augment the authentication afforded by the signature, for example.

Another traditional way to uniquely identify objects is to assign serial numbers, by counting, in a most convenient and orderly fashion. However, traditional serial numbers offer little obstacle to a counterfeiter because he can, for example, assign matching ascending and descending numbers given one correct serial number as a start, thereby duplicating authorized numbers only once. Even if two objects with matching serial numbers were found, thereby finding at least one counterfeit, mechanical techniques may still be required to tell which is counterfeit.

Also, counterfeiters could avoid following a pattern that may be helpful to pursuing authorities if the pattern were discovered. For example, rather than serially numbering their fakes, counterfeiters may randomly select numbering within a wide range of known-to-be valid numbers, so that the possibility of a particular consecutive narrow range of serial numbers being discovered by authorities as having been counterfeited is avoided, making the job most difficult for the authorities (albeit more difficult, but safer, for the counterfeiters as well).

According to described aspects of applicants' invention, intellectual coding techniques may also offer "self-checking" counterfeit detection schemes (serf-checking is a term used with error control coding, adopted for use by applicants when referring to certain intellectual anti-counterfeit coding techniques). Applicants define self-checking as follows: if a single read identifying number does not conform to a secret code, or match up in a database, it must be counterfeit.

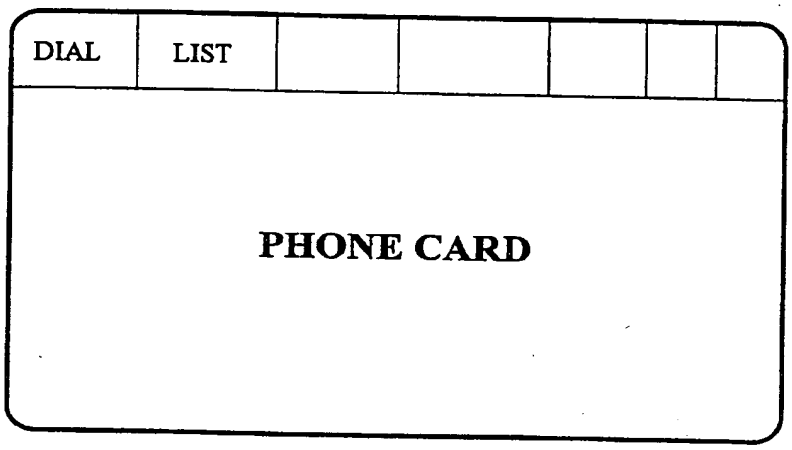

FIG. 22

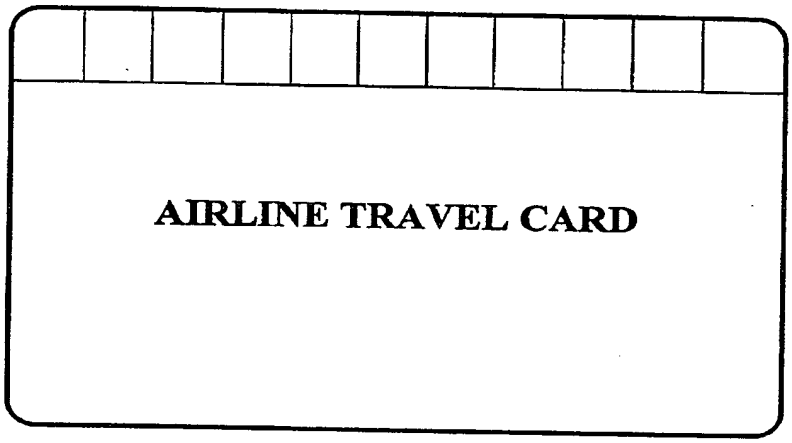

FIG. 23

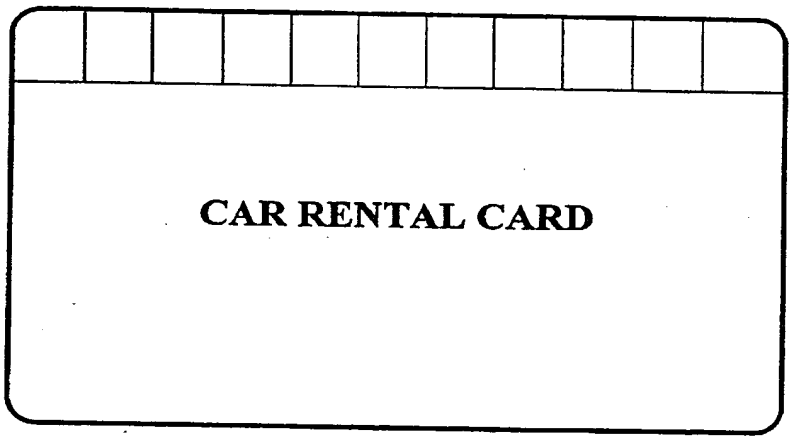

FIG. 24

The use of a secret algorithm is disclosed in McNeight et al's U.S. Pat. No. 4,463,250. MeNeight et at. provides objects with authorized ID numbers that conform to an algorithm or code, so that these ID numbers may be verified or tested for apparent authenticity using the same algorithm. The algorithm is cautiously deployed in locations where it is desirable to detect counterfeit by determining if an object's ID number conforms to the secret algorithm. Caution is required in order to prevent theft or discovery of the algorithm. Authorized ID numbers conform to the algorithm, but the algorithm itself is selected and/or used so that it does not readily allow easy discovery or reverse engineering of the originating algorithm. The algorithm must be kept secret so that it is not also used by unauthorized personnel.

However, if the secret algorithm were to be stolen or discovered (as a computer "hacker" might delight in doing) one may be worse off with the secret algorithm than without, because a false sense of security could have adverse consequences. Consider for example, what if someone unauthorized discovered the secret algorithm but thereafter kept this discovery a secret from those authorized to use the secret algorithm, so that there was no inkling that the secret had fallen into the wrong hands? Genuine objects authorized by the secret algorithm's ID numbers may then be more vulnerable and susceptible to being counterfeited than if traditional serial numbers had been used in the first place.

An encryption algorithmic technique used to calculate security codes is disclosed in Peter White's U.S. Pat. No. 4,630,201. White's invention concerns security for checks and other transactions involving money. White, uses a table of random numbers. The same table of random numbers is associated both with a portable transaction device and with a bank's central processor.

For a check, for example, a random number is selected from the table in the transaction device and used to encode the dollar amount of the particular check using an encryption algorithm. The calculated result, a security code, is then put on the check. The authenticity of the security code on such a check may be verified, by recalculating the security code again, in the same manner, in the bank's central processor, and comparing the two security codes for a match.

SUMMARY OF THE INVENTION

The invention disclosed herein utilizes the underlying principle of uniqueness for counterfeit detection. In accordance with the invention, each genuine object is assigned a different authorized identifying code. Counterfeit is detected when incorrect, repeated or out-of-place ID numbers are found on objects. ID numbers which are associated with objects may be represented in normal alphanumeric characters or otherwise, such as OCR or MICR fonts of alphanumeric characters, decimal characters, or bar coded characters, etc., which are designed to be machine read, and may be visible or substantially transparent.

In particular, an object's identifying serial number may be appended with one or more distinct random portions, positioned to the right of the serial portion, for example, with or without a decimal point (or binary point if binary were being used) or positioned preceding the serial number, or the serial portion may be understood as including one or more random portions, etc.

A truncated security ID number, comprised of a distinct serial number portion and a first random portion, may be used, for example, on the outside of a product package, and a complete security ID number, with a second random portion along with the serial number and said first random portion, used inside a product's packaging (concealing the complete ID number from casual perusal) such as on a product's enclosed return warranty registration card. Each distinct random portion may include one or more randomly selected digits.

Objects of the invention disclosed herein are to protect proprietary product and document integrity, quality, reliability, safety, authenticity and the like, by creating hurdles for would-be counterfeiters, and thereby reducing or eliminating such illegal, dangerous and/or economically devastating

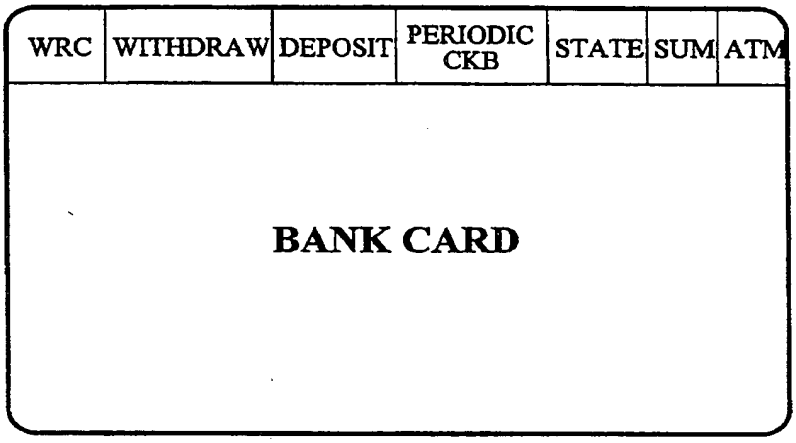

FIG. 19

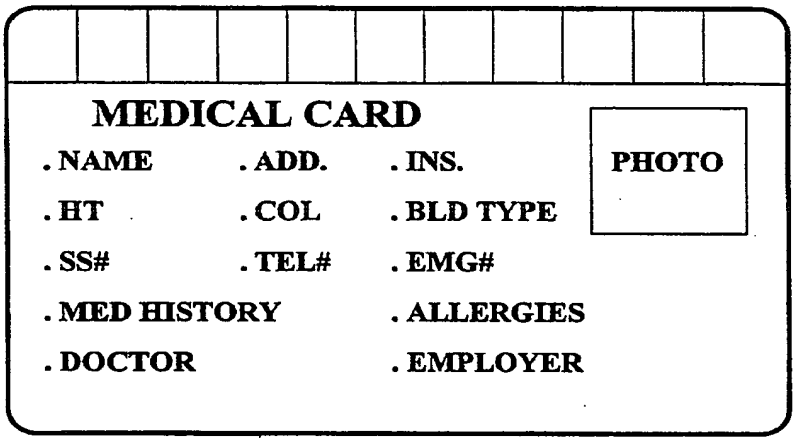

FIG. 20

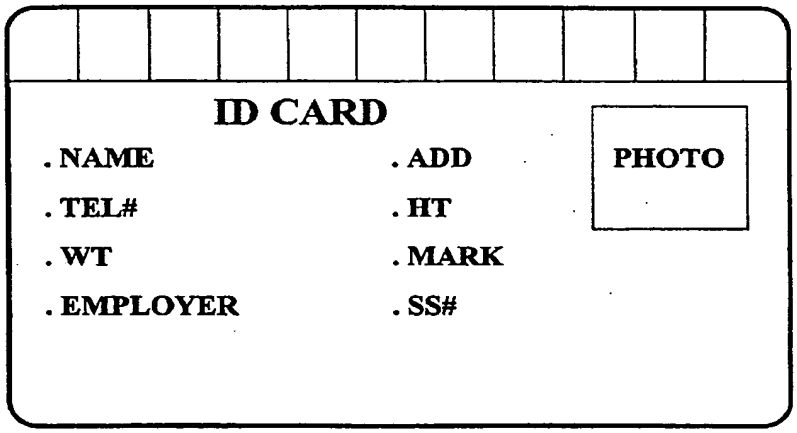

FIG. 21

activity.

In so far as counterfeiting may nonetheless persist, it is another object of this invention to reduce investigative and/or prosecution effort, by providing those pursuing and/or prosecuting counterfeiters with irrefutable evidence, such as products or documents with unauthorized ID numbers, and therefore undeniably counterfeit, so that such culprits can be stopped from foisting their bogus, and typically shoddy, goods on society, and from unfairly competing with more honest commerce.

Other objects of the invention are to improve counterfeit detection and/or deterrence, to apprehend and/or track criminals and/or deter crime.

In accomplishing the above and other objects, individually and in various combinations, the applicants devised coding in accordance with their inventions, particularly but not exclusively for bar codes.

In accomplishing certain of the above objects of the invention, applicants have expanded upon and improved the counterfeit detection techniques disclosed in their U.S. Pat. No. 4,814,589 and copending patent applications mentioned above. According to their invention, such techniques involve accountability, alone or in combination with techniques which make it difficult to copy visually detectable features, such as holograms. The invention may be applicable to almost all types of counterfeitable objects.

In accordance with one aspect of the invention, a method for identifying unauthorized objects is provided comprising: associating with each authorized object identifying information of which at least one portion has been randomly selected; storing said information aside from said association with said authorized objects; reading said information from an object being checked for authenticity; and, comparing said read information with said stored information to detect discrepancy therebetween, whereby an unauthorized object is identified.

In accordance with another aspect of the invention, a method for identifying unauthorized objects is provided comprising: associating identifying coded indicia with each authorized object, a portion of said code having been selected from a detectable series and at least one other portion having been randomly selected; storing said identifying code aside from said association with said authorized objects; reading said coded indicia from an object being checked for authenticity; and, comparing said read coded indicia with said stored identifying code to detect discrepancy therebetween, whereby an unauthorized object is identified.

In accordance with another aspect of the invention, a method for identifying unauthorized objects is provided comprising: on at least one less accessible location of each authorized object, associating identifying information therewith which includes at least two distinct randomly selected portions; on at least one other more accessible location of each authorized object, associating said identifying information therewith but omitting at least one said distinct portion; storing said identifying information with said at least two distinct portions aside from said associations with said authorized objects; reading identifying information from at least one of said locations associated with an object being checked for authenticity; and, comparing said read information with corresponding said stored information to detect one or more discrepancies therebetween, whereby an unauthorized object is identified.

In accordance with this aspect of the invention, said identifying information may be read from both said locations associated with an object being checked for authenticity; and, said read information from both said locations may be compared with corresponding portions of said stored information to detect one or more discrepancies therebetween, whereby an unauthorized object is identified.

In accordance with another aspect of the invention, a method for identifying unauthorized objects with outer covering, such as products with packaging, is provided comprising: on at least one location inside said covering of each authorized object, associating identifying information therewith which includes at least two distinct randomly selected portions; on at least one location on the outside of said covering of each authorized object,

☐ TYPE	☐ PRINT	☐ ERASE
☐ HELP	☐ SEC	☐ ←
☐ ↑	☐ ↓	☐ →
☐ SUMMARY	☐ ACCT/PAY	☐ WEEKLY
☐ MONTHLY	☐ YEARLY	☐ LAST USED
☐ CREDIT LIMIT	☐ BALANCE	☐ LOAD PC
☐ WRITE CHECKS	☐ WITHDRAW	☐ DEPOSITS
☐ PERIODIC CHECKS	☐ STATEMENT	☐ ATM
☐ WRITE/TYPE	☐ SEARCH	☐ REMIND
	☐ SPECIAL COMMANDS	

FIG. 18

associating said identifying information therewith but omitting at least one said distinct portion; storing said information with said at least two distinct portions aside from said associations with said authorized objects; reading identifying information from at least one of said locations associated with an object being checked for authenticity; and, comparing said read information with corresponding said stored information to detect one or more discrepancies therebetween, whereby an unauthorized object is identified.

In accordance with this aspect of the invention, said identifying information may be read from both said locations associated with an object being checked for authenticity; and, said read information from both said locations may be compared with corresponding portions of said stored information to detect one or more discrepancies therebetween, whereby an unauthorized object is identified.

In accordance with another aspect of the invention, a method of designating an object as authorized is provided comprising: randomly selecting at least one digit; storing said digit with a serial number for said object; and, associating said serial number and digit with said object.

In accordance with another aspect of the invention, a method of designating an object as authorized is provided comprising: providing at least one digit that cannot be anticipated; storing said digit with a serial number for said object; and, associating said serial number and digit with said object.

In accordance with yet another aspect of the invention, a method of designating an object as authorized is provided comprising: randomly selecting at least two distinct digits; storing said two distinct digits with said authorized object's serial number; and, associating said serial number and one distinct digit of said two distinct digits with said object on the outer surface thereof; and, associating said serial number and said two distinct digits with said object inside the outer surface thereof.

In accordance with still another aspect of the invention, a method of designating an object as authorized is provided comprising: randomly selecting at least two distinct digits; storing said two distinct digits with said authorized object's serial number; and, associating said serial number and one distinct digit of said two distinct digits with said object on the outer surface thereof.

In accordance with this aspect of the invention, said serial number and said two distinct digits may be located inside said object's outer surface. Also in accordance with this aspect of the invention, said serial number and said two distinct digits located inside said object's outer surface may be associated with a return card for said object.

In connection with one or more objects of the invention or aspects of the invention described herein, said identifying information may include a plurality of randomly selected portions, and at least one said randomly selected portion may be concealed in a given condition of said object. e.g., when wrapped in its original packaging.

Also in connection with one or more objects of the invention or aspects of the invention described herein, said identifying information may be: machine readable, represented at least once in machine readable code elements, and/or, represented at least once in a bar code symbol,

When said authorized objects with said associated identifying information in a bar code symbol also have UPC symbols associated therewith, said identifying information in a bar code symbol and said UPC symbol may be located near each other, and/or a reading from one of said symbols near each other is automatically delayed until said other symbol is also read in the same reading operation, and/or one bar code symbol is associated with said object, another possible bar code symbol not being near to said one, and said one bar code symbol is automatically read without undue delay in the reading operation due to anticipation of said another possible bar code symbol being near to said one, and/or said identifying information in a bar code symbol located near said UPC symbol may be substantially transparent, and/or said substantially transparent identifying information in a bar code symbol may be placed right over said UPC symbol.

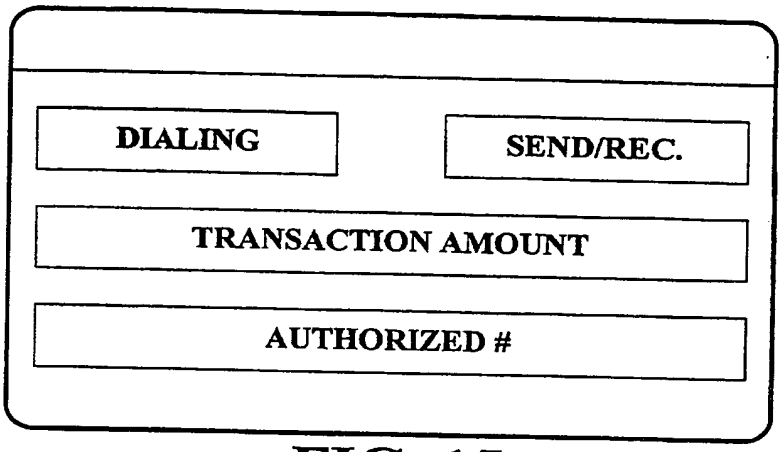

FIG. 15

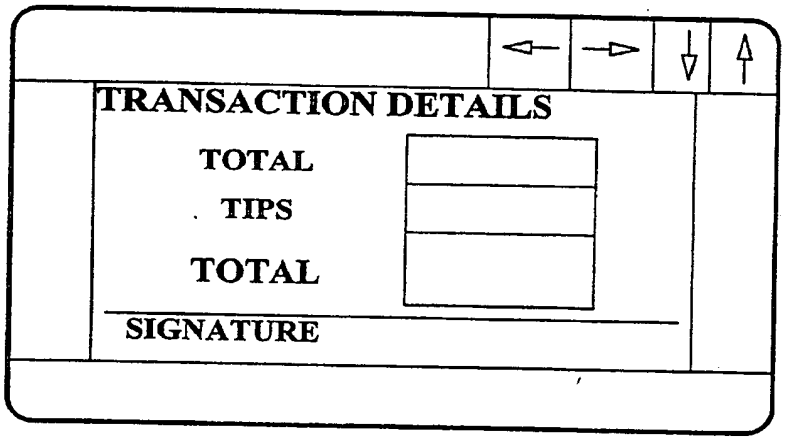

FIG. 16

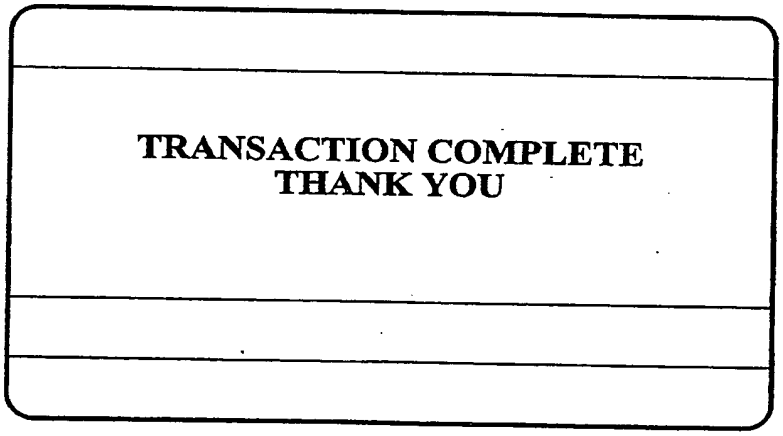

FIG. 17

Also in connection with one or more objects of the invention or aspects of the invention described herein, said read information may be checked to determine if the same identifying information was previously read from another similar object, whereby at least one of the objects with said same identifying information may be identified as an unauthorized object, and/or said same identifying information may be flagged or stored in a list to facilitate identification of additional possible unauthorized objects with said same identifying information, and/or a said object's read identifying information may be checked to see whether it has been previously flagged or stored in a list, whereby an unauthorized object may be identified.

Also in connection with one or more objects of the invention or aspects of the invention described herein, each said object may have associated therewith an other object which may be separated from said object and with which corresponding respective said identifying information having at least one randomly selected portion may be associated. Said other object may be a return card. Said corresponding identifying information may be read from a said return card and compared to said stored information to detect discrepancy, whereby an unauthorized return card may be identified.

Also in connection with one or more objects of the invention or aspects of the invention described herein, said identifying information associated with an authorized object may also include at least one other portion which has been selected in accord with a secret algorithm.

In accordance with yet another aspect of the invention, a system is provided for automatically detecting an unauthorized object, each authentic object having associated therewith authorized information of which at least one portion has been randomly selected, the system also comprising: means for storing said authorized information; means for reading information from an object; and, means for automatically detecting when said read information does not match up to said stored authorized information, whereby an unauthorized object is detected.

In accordance with another aspect of the invention, a system is provided for identifying an unauthorized object from a set of authorized objects, each authorized object of said set having identifying information associated therewith of which a portion has been calculated using an algorithm dependent on a randomly selected number, the system comprising: means for securely storing said randomly-selected numbers at a single location only; means for reading identifying information from an object: means coupled to receive said information read from said object for at least temporarily storing that information; and means for automatically detecting when information read from any object includes a different said portion than that calculated using said algorithm, whereby an unauthorized object is identified.

In accordance with another aspect of the invention, a system is provided for identifying an unauthorized object from a set of authorized objects, each authorized object of said set having identifying information associated therewith of which a portion has been calculated using an algorithm dependent on a randomly selected number, the system comprising: means for securely storing said identifying information, including said calculated portion, aside from said authorized object; means for reading identifying information from an object; means coupled to receive said information read from said object for at least temporarily storing that information; and means for automatically detecting when information read from any object includes a different said portion from said securely stored identifying information, whereby an unauthorized object is identified.

In connection with one or more objects of the invention or aspects of the invention described herein, means may be provided for automatically erasing randomly selected numbers for security purposes, and/or means may be provided for securely storing identifying information only at a single location aside from authorized objects, and/or means may be provided for automatically erasing a portion calculated using said algorithm after association with authorized objects.

In accordance with yet another aspect of the invention, a plurality of genuine essentially identical objects are provided, each having authorized identifying information associated therewith, the associated information

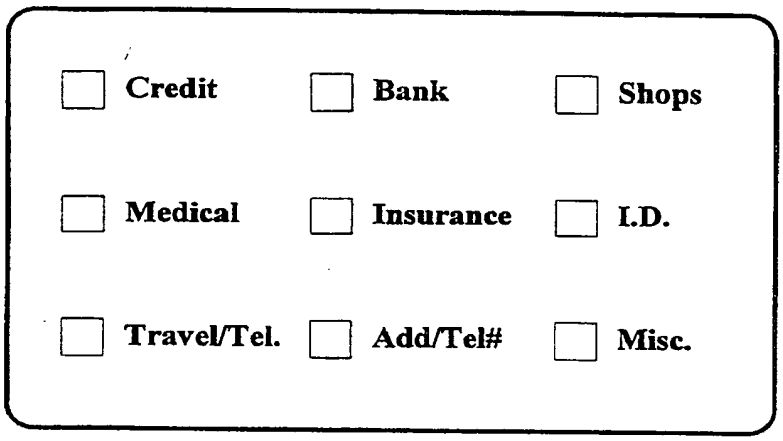

FIG. 12

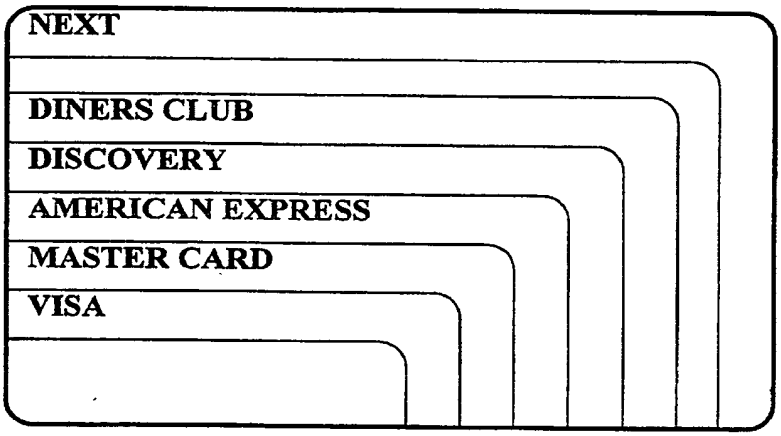

FIG. 13

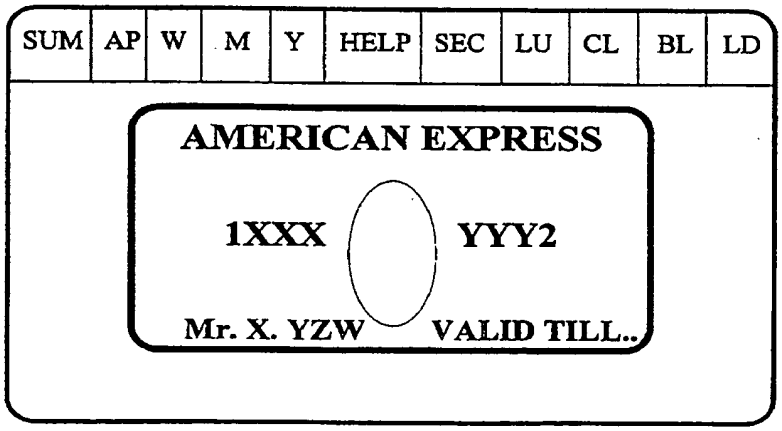

FIG. 14

being useful for indicating authenticity of each object, this information including a distinct serial number portion comprised of at least enough digits to uniquely identify each said object, and a second portion that cannot be anticipated, this second portion having at least one digit. This one digit may be randomly selected or result from a calculation using at least one randomly selected digit. Aside from association with said objects said information may be stored along with respective randomly selected digit(s) or second portions.

A system for indicating authenticity of such objects is also provided and it includes such objects and means for storing information aside from the association with objects, means for reading information from an object, means for comparing read information with stored information and finding a match therebetween, a match between read information and stored information indicating that the object with such read information is authentic.

In accordance with yet another aspect of the invention, a method of designating at least one of many essentially identical and identifiable objects as authorized is provided comprising: providing a serial number for one such object; and, providing a randomly selected number for this one object: using at least one digit of said serial number and at least one digit of said randomly selected number with an algorithm to calculate another number that cannot be anticipated for said object; and, associating at least one digit of said number that cannot be anticipated with said object.

In accordance with yet another aspect of the invention, a plurality of genuine essentially identical objects are provided, each having authorized identifying information associated therewith, this associated information being useful for indicating authenticity of each said object, and this information includes at least one digit that cannot be anticipated.

A system for indicating authenticity of such objects is also provided and it includes such objects and means for storing said information aside from said association with said objects; and, means for retrieving said stored information; and, means for reading information from an object; and, means for comparing said read information with said retrieved information and finding a match therebetween, a match indicating that said object with said read information is authentic.

Another system for indicating authenticity of such objects is also provided and it includes such objects and means for storing said identifying information aside from said association with said objects; and, means for storing other information related to said identifying information; and, means for retrieving said stored identifying information; and, means for retrieving said stored related information; and, means for reading information from an object; and, means for comparing said read information with a result of a calculation using said retrieved related information, and finding a match therebetween, a said match indicating that said object with said read information is authentic.

The invention and its background are described with particular reference to ID numbers, and bar coded ID numbers, in decimal, base ten, but which may be represented in any base such as binary, ternary, octal, decimal, base 43, etc. However, the invention has wider application and it is not intended to limit the scope of the invention by such references.

DRAWING DESCRIPTION:

DESCRIPTION OF THE DRAWINGS

The invention is illustrated by way of example and not limitation in the figures of the accompanying drawings in which like references, if any, indicate like parts, and in which:

FIG. 1 is a plan view of a product return card with ID number indicia in decimal digits and in bar code. The product return card may be found inside a product package. The ID number indicia include two random portions, shown as 23 and 17.

FIG. 2 is a side view of the outside of a product package with ID number

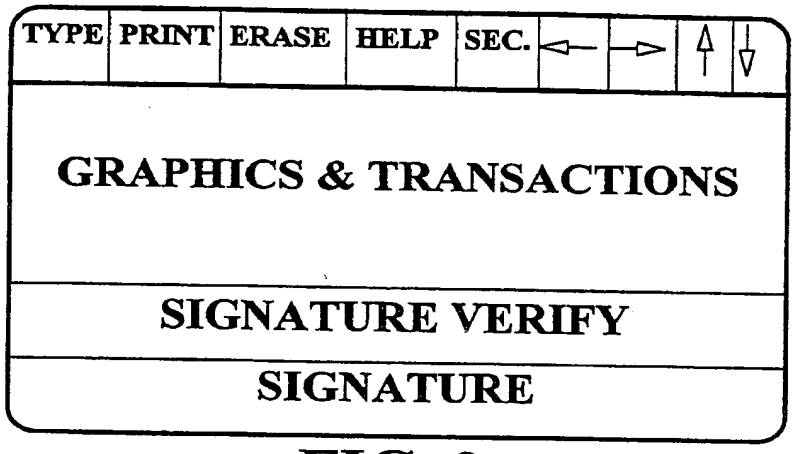

FIG. 9

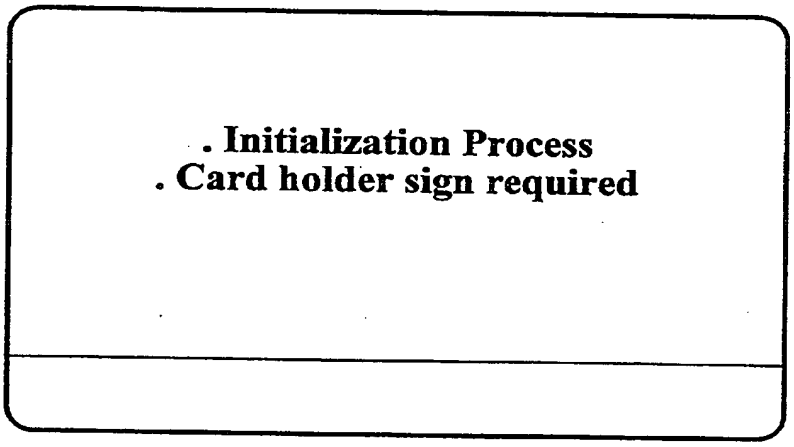

FIG. 10

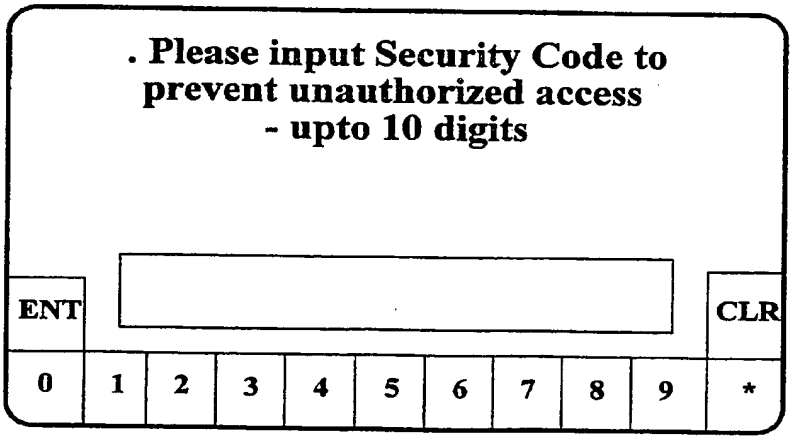

FIG. 11

indicia thereon corresponding in part to the ID number indicia on the product return card of FIG. 1.

FIG. 3 is a side view of the outside of a product package with ID number indicia thereon corresponding in part to the ID number indicia on the product return card of FIG. 1. Also located on this same outside side near said ID number indicia is a standard UPC bar code symbol.

FIG. 4 is a view of a product package with transparent or invisible to the naked eye ID number information and a standard UPC bar code symbol superimposed relative to each other.

DETAILED DESCRIPTION:

DETAILED DESCRIPTION

Many products already include registration material, such as a blank name, address, where purchased form, printed on a return postcard on which may be found the product's ID number. Such cards are often used to activate a product's warranty.

Counterfeit products may be detected by looking for duplicate registration of normal serial numbers. However, this procedure leaves something to be desired, because counterfeit cannot be detected via the serial number until two (or more) of the same serial numbers are eventually registered, and even so, when two of the same serial numbers do turn up, an investigation must first be made to determine if one is genuine (as both may be fake) and if so, which one. Also, assuming a counterfeit product is positively detected and the vendor who sold the counterfeit product is identified by the product registrant, it may still be impossible, or cumbersome at best, to determine if other products in the vendor's stock are also counterfeit. Further, physical examination procedures would likely be "intrusive" and may render examined products unfit for retail sale.

In a way, these difficulties arise from the use of traditional serial numbers. Because traditional serial numbers are as orderly and convenient to use as possible, they are also completely and readily predictable, and thus are directly vulnerable and susceptible to being counterfeited.

Applicants' telling anti-counterfeit technique overcomes these short-comings: registration involving just one ID number on a counterfeit product can immediately and unmistakably be identified as fake, and even before a "lead" from the registration process, counterfeit products can be positively identified on the retail shelf or in mail order inventory warehouses or distribution channels, etc., without opening the product's packaging.

According to the invention, ID numbers include a serial portion and one or more random portions appended to, or associated with, the serial portion. Such D numbers have the serial portion in predefined digit positions, so that ID numbers may be used just as orderly and conveniently as traditional serial numbers. The serial number portion (which may be called the serial field) of the ID number is appended with one or more random portions (each random portion may be called a random field). Each random portion may contain one or more randomly selected digits. A random number generator may be used which may, e.g., randomly select digits based on cosmic noise. Required randomly selected numbers may be provided on-the-fly, as needed, and then stored if required or erased if not required. Or, required randomly selected numbers may be generated and stored in a list and the list then referred to as required. It may be useful for random portions to be separated from the serial portion by a decimal point, for example.

Security is enhanced because such complete authorized ID numbers are unpredictable as follows: if one decimal digit is randomly selected, only one in ten ID numbers would be predictable by a counterfeiter, and if two digits are randomly selected, only one in a hundred, etc. There is no secret code to be stolen or discovered. With applicants' random technique, the problems and worries described above for traditional serial numbers and ID numbering in accord with a secret algorithm are simply avoided.

For example, the serial random number (SRN) shown on the Product Return Card

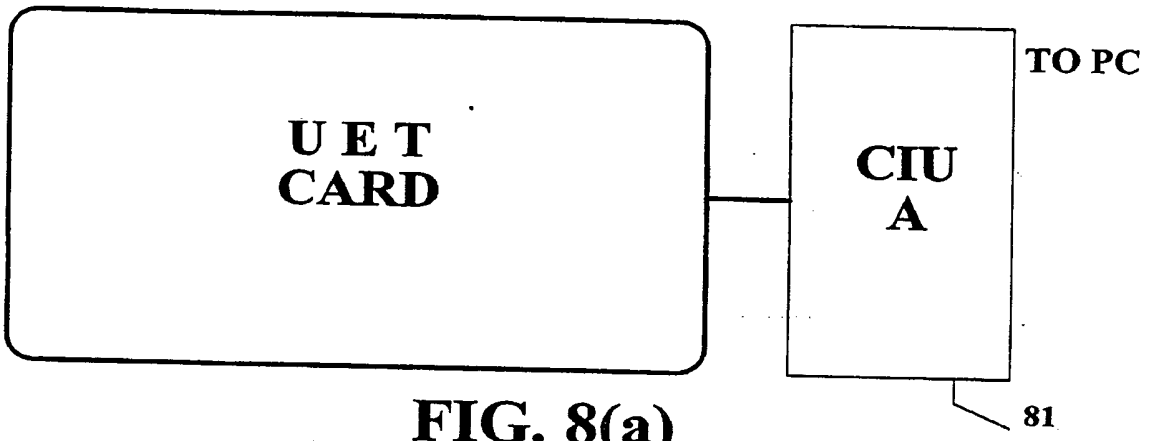

FIG. 8(a)

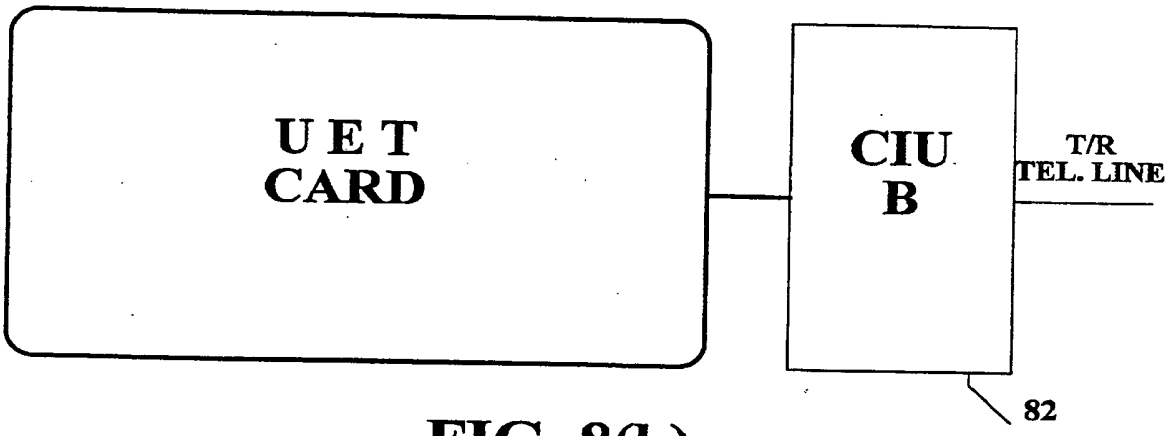

FIG. 8(b)

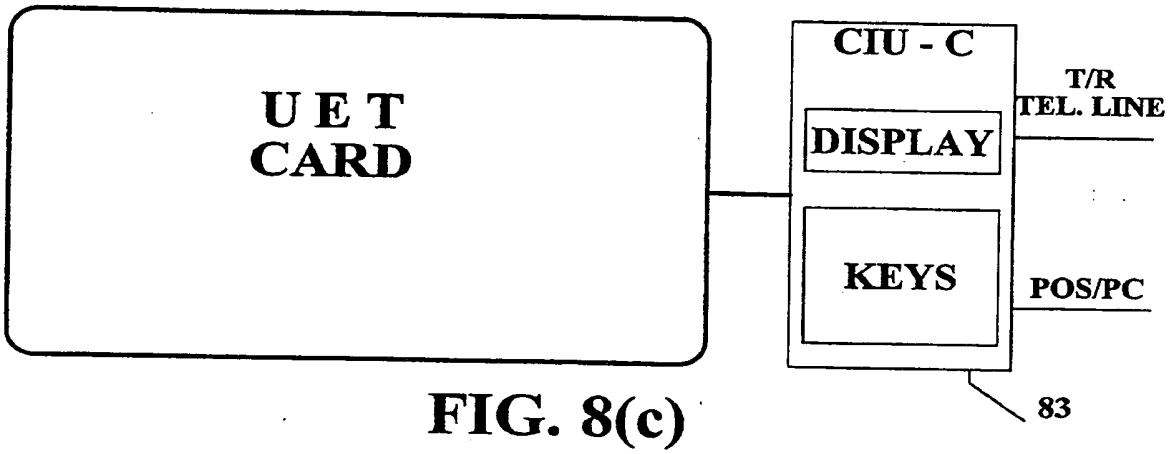

FIG. 8(c)

in FIG. 1 is:

123456 23 17

For example, this ID number, 123456 23 17, is associated with a genuine product. The first six digits of the ID number, 123456, comprise a traditional sequential serial number with sufficient range to uniquely identify one million genuine products, from 000000 to 999999. The next four digits, in this example 23 and 17 (shown throughout herein with separating spaces for clarity) are randomly selected, and stored in a file, such as a computer file, perhaps a file associated with a database system, along with the traditional serial number portion, to form a file listing of complete authorized ID numbers. In other words, aside from associating authorized ID numbers with authentic objects, authorized ID numbers are also stored separately, e.g., on a list stored in a computer file. Because of the serial portion, the list of complete authorized ID numbers is as orderly as can be, and because of the randomly selected parts, it is also unpredictable as described.

For example, when a product's ID number, e.g., 123456 23 17, is entered from the return card in a product registration system computer containing the listing of complete authorized ID numbers, the random digits can be checked automatically--if they do not all match those which were originally stored, a counterfeit product's unauthorized ID number is positively and immediately detected. The product registration system computer may also be used by investigators looking for counterfeit, without need for registration and/or return cards, as described below.

In this aspect, complete authorized ID numbers simply cannot be effectively predicted or anticipated without one-for-one copying from complete genuine ID numbers by the counterfeiter, which is prohibitive, or, at least severely limiting, creating a hurdle for the counterfeiter.

Corresponding ID numbers, or preferably ID numbers corresponding only in part, may also be put on the outside of product packaging. The truncated serial random number (SRN), which corresponds in part to the ID number indicia shown in FIG. 1, is shown in FIG. 2 on the Product Package as:

123456 23

The reason for truncation is described below. Use of such ID numbers on the outside of product packaging makes them readily accessible, and allows a "shopping" service contracted by the product's manufacturer, or an investigator, to read and store bar coded ID numbers from products, e.g., on store shelves, and then send them, for example using a modem, to the manufacturer's system registration computer where the randomly selected portion of the ID numbers read from products can be checked against the stored list of complete authorized ID numbers, so that unauthorized ID numbers from counterfeit products may be detected. Thus, counterfeit products may be identified even before customer purchase, and authorities may be put on the trail of the perpetrators sooner. In enforcement proceedings, even good leads can get cold.

Or for example, applicants' counterfeit product detection system could be set up to include handheld devices that combine radio communication capability with bar code reading (e.g., the LRT 3800, which also includes portable computer terminal capabilities, in a handheld unit, a product of Symbol Technologies Inc., of Bohemia, N.Y.) so that counterfeit could be detected at about the speed of light while an investigator points the device at a product being checked for authenticity. For example, the LRT 3800 device reads and interprets the ID number bar code on a product that may be counterfeit, radio communicates this information to the product registration system computer to automatically check the ID number's random digit(s) to see if they match what was originally stored, and then receives back from the computer an indication if the ID number is unauthorized, thereby detecting counterfeit.

The type of equipment used by Federal Express delivery service may be adapted for applicants' counterfeit detection system. Federal Express uses bar code reading and communication devices, and sometimes a communication satellite, in a package tracking system (see Automatic ID News Vol. 7, #2, 2/91, pg. 16). With such devices working with a central anti-counterfeit computer

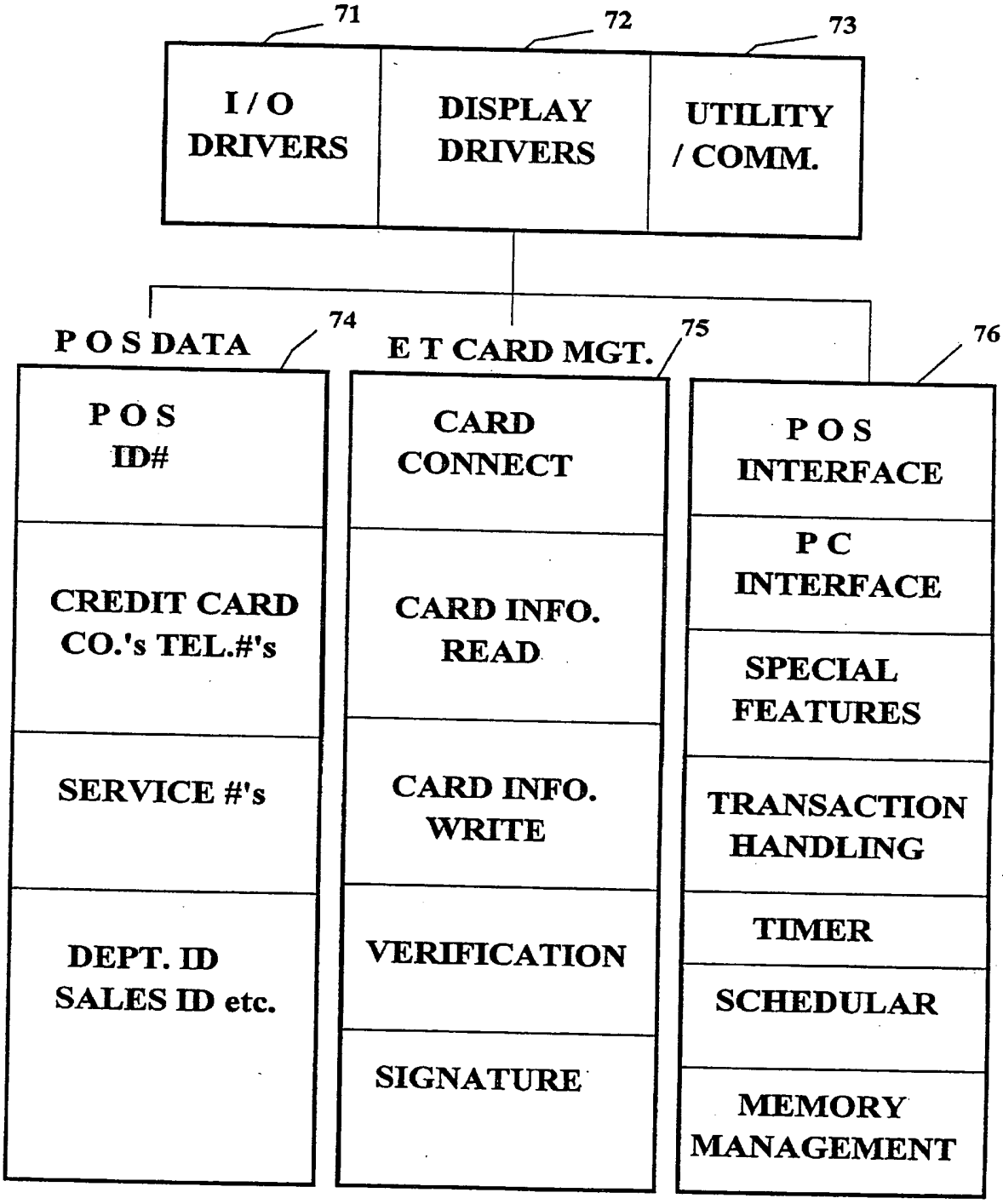
71
72
73
I / O DRIVERS
DISPLAY DRIVERS
UTILITY / COMM.
P O S DATA
74
E T CARD MGT.
75
76
P O S ID#
CREDIT CARD CO.'s TEL.#'s
SERVICE #'s
DEPT. ID SALES ID etc.
CARD CONNECT
CARD INFO. READ
CARD INFO. WRITE
VERIFICATION
SIGNATURE
P O S INTERFACE
P C INTERFACE
SPECIAL FEATURES
TRANSACTION HANDLING
TIMER
SCHEDULAR
MEMORY MANAGEMENT

FIG. 7

system, for example, counterfeit could be detected quickly, on a shelf in a location being checked for having counterfeit product, at a U.S. border in a routine or special Customs inspection, and so forth.

If a counterfeit product with an unauthorized ID number did turn up in the registration process, a shopping service or an investigator could be dispatched directly to the location that sold the counterfeit and/or to this seller's supplier, to check for additional counterfeit products, without opening product packaging. Such investigation may be conducted covertly if there is suspicion that the vendor himself may be implicated. (Bar code readers with storage, for example, only the size of a credit card, are commonly available.)

With bar coded ID numbers on the outside of packages, investigative effort is reduced, and subsequent prosecution effort may be simplified, because prosecuting attorneys may have irrefutable evidence: e.g., product with an unauthorized ID number, and therefore counterfeit.

Dual Random

ID numbers located on the outside of packaging are more accessible than ID numbers located inside the packaging, and may therefore more readily allow the possibility of a counterfeiter acquiring authorized ID numbers from the outside of genuine product packaging than from the inside (this may not be a significant risk in all cases). For example, a counterfeiter might bribe someone in a distributor's shipping/receiving department to accumulate "outside" authorized ID numbers with a concealable bar code reader so that they could be used later on counterfeit products. if this happened, the manufacturer could be back where he started, looking for duplicates, suffering the shortcomings mentioned above, or perhaps even being worse off because of a false sense of security.

Applicants' anti-counterfeit invention anticipates this possibility. For example, the complete authorized ID number, 123456 23 17, is printed on the return registration card (as shown in FIG. 1) which is located inside the package and is therefore less accessible than the ID number located on the outside of packaging, thus concealing the complete authorized ID number from casual perusal. For example, if a product is in its original packaged condition, an ID number with associated random portions located inside the packaging would be concealed.

Only a truncated authorized ID number, 123456 23, is printed on the outside of the package (as shown in FIG. 2). Thus, even if a counterfeiter surreptitiously acquired outside ID numbers from product packaging, counterfeit products can still be detected immediately upon registration, and also with absolute certainty, and still without relying on the appearance of duplicate registration ID numbers.

If the first two random digits of inside ID numbers are correct, and only the last two random digits are wrong, the manufacturer need not go looking for incorrect outside ID numbers on any shelves, so to speak, because it is evident that the counterfeiter somehow acquired authorized (but truncated) outside ID numbers.

In this case the manufacturer is still not without help from the system computer, by which this discovered "leak" may be dealt with, and this now notorious counterfeiting ring broken. Indeed, it may well be possible to catch culprits "in the middle," by analyzing when the products with the copied outside ID numbers were manufactured and through what distribution channels they moved, as well as backtracking the source of the counterfeit product itself.

In an embodiment of applicants' invention, a list (e.g., a partial listing limited to specific ranges of serial numbers, and/or selected geographical and/or chronological parameters, etc.) of authorized outside ID numbers in the above example, 123456 23) might be supplied in a portable, noncommunicating unit to investigators for use in the field as described below. For increased security, perhaps specially trusted investigators only would be supplied with such "portable" lists, and/or such lists may only be supplied just prior to an investigation at a given location, and/or such lists may only be supplied in units that automatically erase the list after a

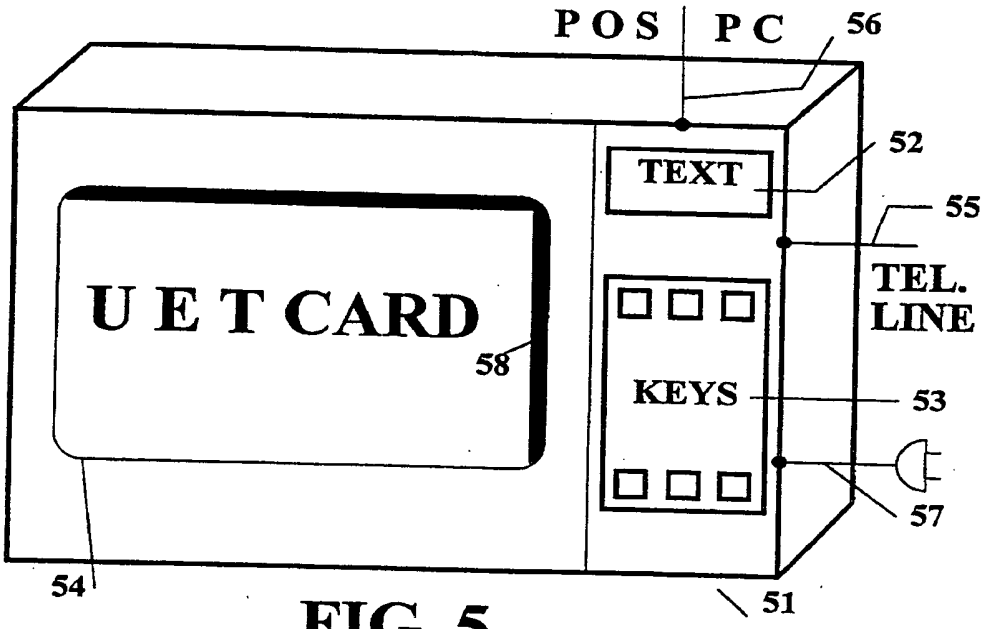
POS
PC
56
52
TEXT
55
TEL.
LINE
U E T CARD
58
KEYS
53
57
54
51

FIG. 5

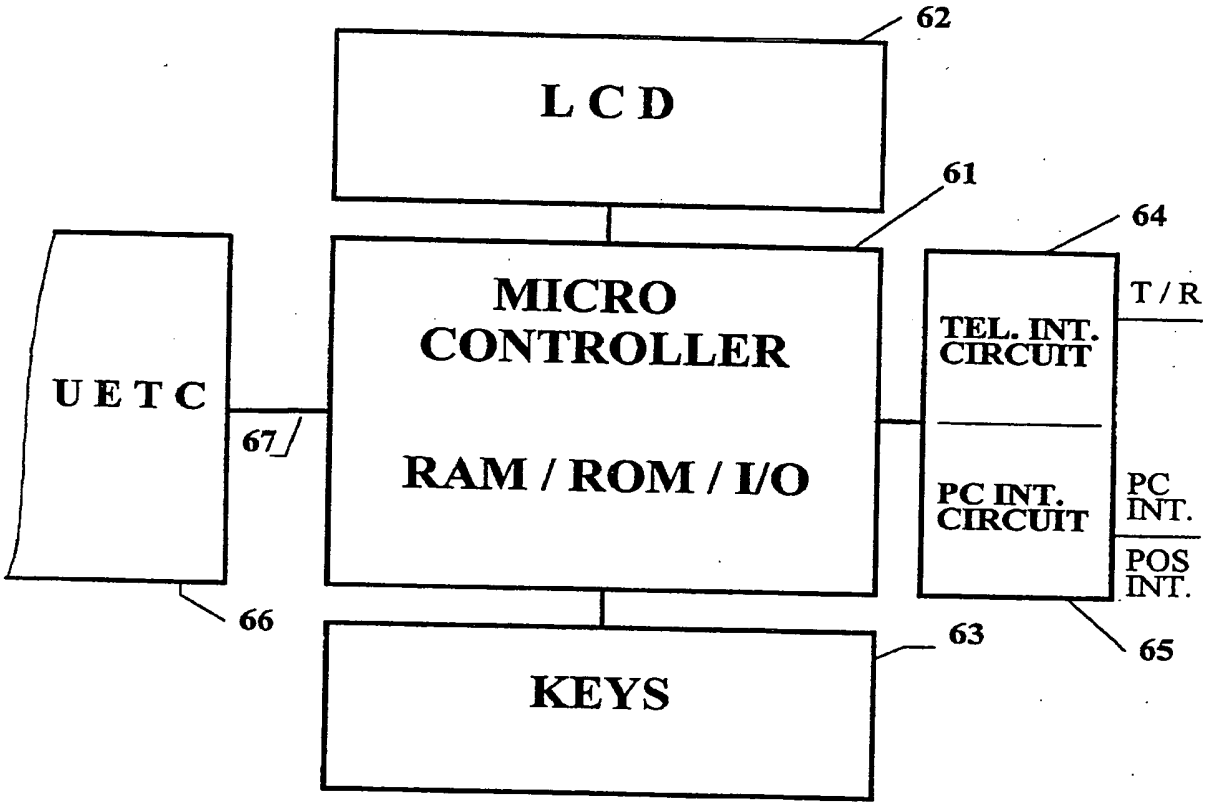
62
L C D
61
64
MICRO
CONTROLLER
RAM / ROM / I/O
T / R
TEL. INT.
CIRCUIT
PC INT.
CIRCUIT
PC
INT.
POS
INT.
U E T C
67
66
63
65
KEYS

FIG. 6

given amount of time has elapsed and/or at a specified time, etc.

In any case, this embodiment is less of a security exposure than supplying complete ID numbers for use in the field, especially if only a limited, partial listing is provided. For example, even if a portable list was acquired and used by counterfeiters, more complete ID numbers, such as those from a return card, would still expose the crime.

For example, with portable lists counterfeit objects may be detected immediately, in the field, by comparing ID numbers read from a product's packaging directly against the list to determine if the correct random field for a respective serial number field is present on a product's package, without checking with the central computer where the master list of complete ID numbers is stored, on-site so to speak, no communications required, using a portable unit (much as checking a hot list, described below). Thus, increased convenience, effectiveness and cost saving (e.g., limited communication requirements) may be realized when looking for counterfeit, without undue security exposure.

Security Enhancements

Additional security enhancements are possible. For example, to prevent unauthorized copying of ID numbers, a return card's complete ID number, or just the random security part(s), may also be concealed, e.g., with latex covering, like the VIRN number (Void If Removed Number) on an instant lottery game ticket, or the ID number may only be represented on the card in a customized "secret" bar code format.

Variations are possible. For example, if the possibility of a counterfeiter acquiring outside ID numbers during distribution exists, and return cards are not appropriate for a given product line, several such products may be packed for shipping in a sealed carton concealing the products' outside ID numbers during distribution.

Also, outside ID numbers can be put on such cartons, and latex-covered return from the retail vendor cards can be put in the carton (but not inside individual product packaging).

And, as described below, the use of, e.g., 123456 17 instead of 123456 23 17 on a return card, adds security.

Four Random Fields

In another example, consider an ID number with four appended random fields:

123456.sub.-- 23 17 79 10

The blank digit position shown with an underline is described below. 123456 23 may be put on the outside of a shipping carton containing ten products. 123456 23 17 may be latex-covered and put on a return from the retail vendor card and located inside the carton, but not inside individual product packaging.

Ten ID numbers using 123456.sub.-- 23 17 79 may be used as follows, one on the outside of each product package:

1234560 23 17 79

1234561 23 17 79

1234562 23 17 79

1234563 23 17 79

1234564 23 17 79

1234565 23 17 79

1234566 23 17 79

1234567 23 17 79

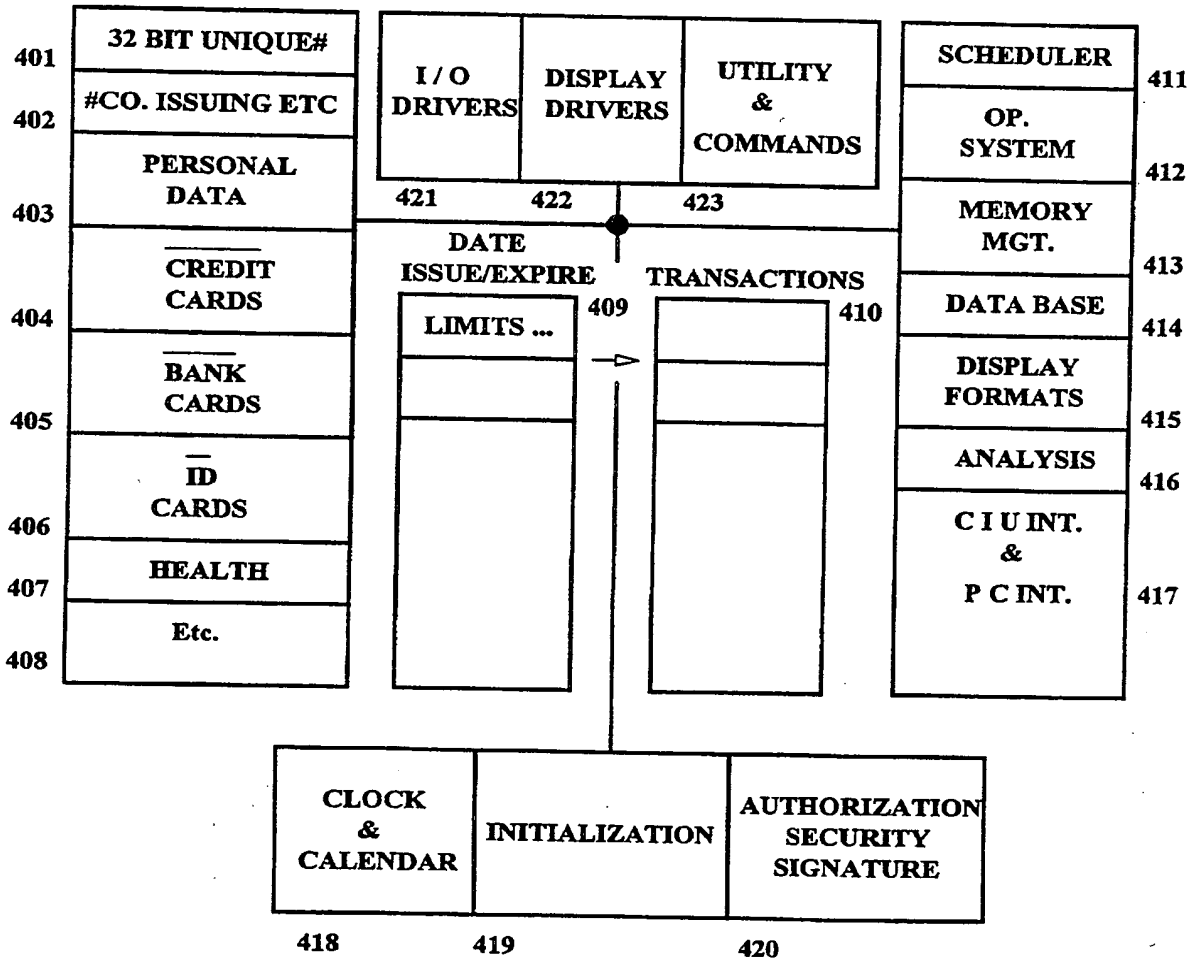
401
32 BIT UNIQUE#
402
#CO. ISSUING ETC
403
PERSONAL DATA
404
CREDIT CARDS
405
BANK CARDS
406
ID CARDS
407
HEALTH
408
Etc.
I / O DRIVERS
DISPLAY DRIVERS
UTILITY & COMMANDS
421
422
423
DATE ISSUE/EXPIRE
LIMITS ...
409
TRANSACTIONS
410
SCHEDULER
411
OP. SYSTEM
412
MEMORY MGT.
413
DATA BASE
414
DISPLAY FORMATS
415
ANALYSIS
416
C I U INT. & P C INT.
417
CLOCK & CALENDAR
INITIALIZATION
AUTHORIZATION SECURITY SIGNATURE
418
419
420

FIG. 4

1234568 23 17 79

1234569 23 17 79

Each may be applied to ten respective product package's outside. The additional digit in each of these ID numbers (in the seventh position from the left, shown underlined) uniquely identifies each of the ten products, for the batch serial number 123456, and may conveniently be considered as part of the serial number portion of the ID number for individual products. Each product may also have a return card inside its packaging, each with one of the following ID numbers:

1234560 23 17 79 10

1234561 23 17 79 10

1234562 23 17 79 10

1234563 23 17 79 10

1234564 23 17 79 10

1234565 23 17 79 10

1234566 23 17 79 10

1234567 23 17 79 10

1234568 23 17 79 10

1234569 23 17 79 10

If this type of embodiment were used, one risk is that a savvy counterfeiter obtaining one correct ID number from a return card, such as 1234567 23 17 79 10 in this example, might correctly deduce nine other authorized ID numbers, those others between: 1234560 23 17 79 10 and 1234569 23 17 79 10, inclusive.

Because of the difference in the number of digits in ID numbers for respective locations, when ID numbers are read it may readily be automatically determined by apparatus where that ID number was read from, whether from the outside of the carton of ten products, from inside the carton on the carton's return card, from on the outside of an individual product or from the return card inside the individual product package.

In the event of counterfeiting of authorized ID numbers such as these, knowledge of which random digits have been copied provides useful information, e.g., when and/or from where the ID numbers were copied. For example, if:

1234560 23 17 79 86

(and other similarly constructed ID numbers) were found on a counterfeit product, a counterfeiter learned correct ID numbers for three places: the outside of the carton, inside the carton, on the outside of an individual product, but not for the product's return card. This would indicate that the counterfeiter had access to the outside of the products' individual packaging for copying, since all random digits up to that point are correct.

However, in some embodiments it may be preferred to increase security. For example, additional security may be realized if the random fields are used more sparingly. For example, while 123456 23 may be used on the outside of the carton of ten products, only 123456 17 may be used on the carton's return card (instead of 123456 23 17). 1234560 79 (the first of ten similar ID numbers corresponding to the above) may be used on the outside of an individual product, and 1234560 10 (again, the first of ten) used on the return card inside an individual product package. Now, for example, knowledge of a valid ID number from the outside of an individual product, 1234560 79 in this example, does not inform of the corresponding random field for the outside of the carton of ten such products (23), or of the corresponding

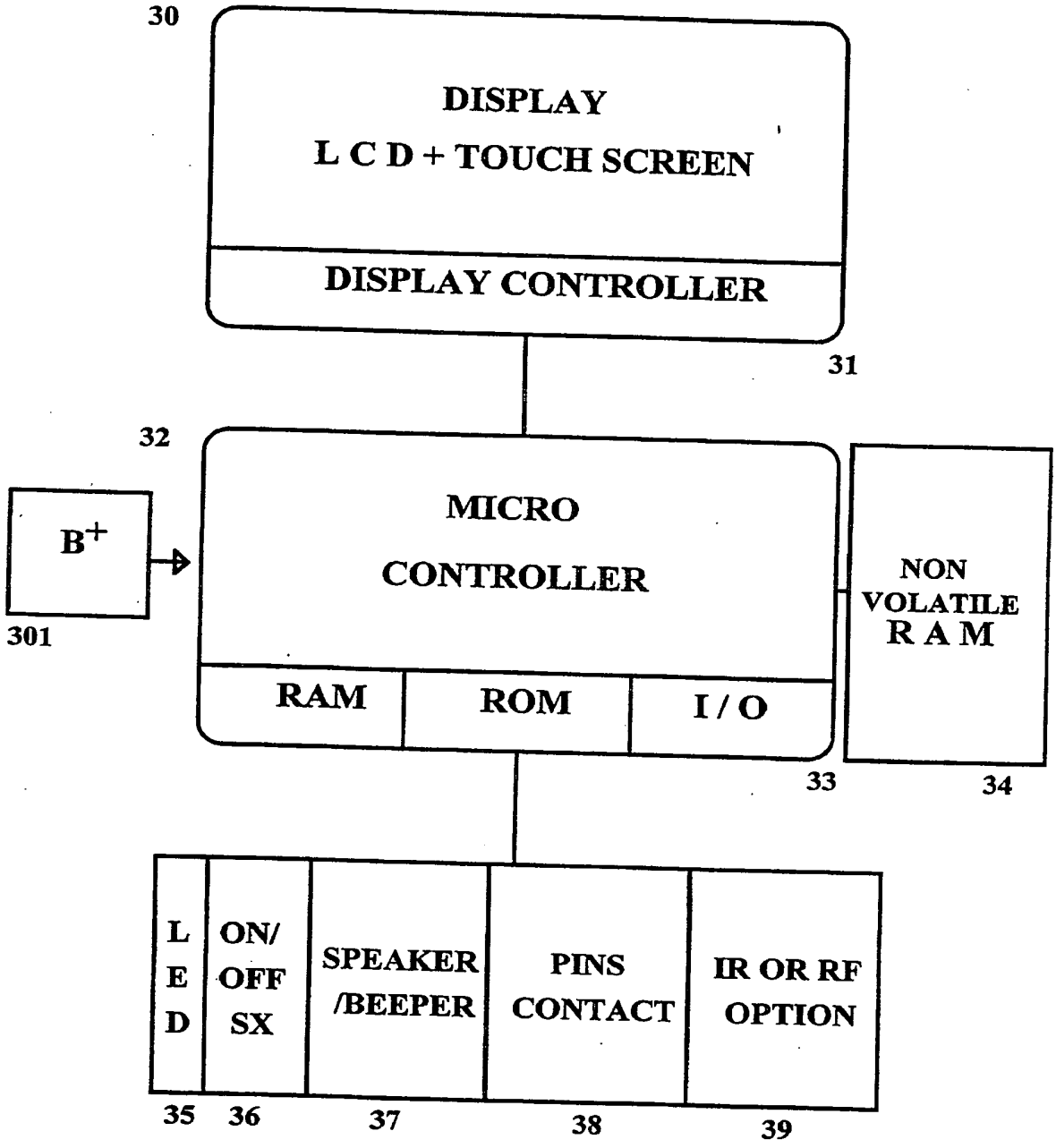
30
DISPLAY
L C D + TOUCH SCREEN
DISPLAY CONTROLLER
31
32
B+
301
MICRO
CONTROLLER
RAM
ROM
I / O
33
NON
VOLATILE
R A M
34
L
E
D
ON/
OFF
SX
SPEAKER
/BEEPER
PINS
CONTACT
IR OR RF
OPTION
35
36
37
38
39

FIG. 3

random field used inside the carton on the carton's return card (17). Thus, higher security is realized.

However, in this example of higher security, inquiries made in the system computer to check an ID number for authenticity, i.e., whether or not the random field digits are correct, would need to inform from where the ID numbers were read. For example, while 123456 23 is correct for the outside of a carton of ten products, 123456 17 is incorrect. 123456 17 read from the wrong location (the outside of a carton) would be an unauthorized ID number and indicate counterfeit.

In another embodiment, say the following ID number (with a sixteen digit serial field and five fields of two randomly selected digits each):

1234567812345678 23 17 79 10 55

were used for documents, for example, on U.S. currency. A file with the serial number portions and only the associated first random field, shown with 23 in this example, may be provided by the Bureau of Engraving and Printing to commercial banks for their general use in detecting counterfeit, a file of the random fields 23 17 provided to Federal Reserve Banks for their use, a file of the random fields 23 17 79 to the Treasury, FBI, CIA, etc., a file of the random fields 23 17 79 10 may be used exclusively by those most trusted in the Secret Service, and a file of all five random fields, 23 17 79 10 55 may be stored for safe keeping and used with extreme caution only if ever needed. In this manner, if sophisticated counterfeiting were to occur, authorities would know exactly where to start looking for culprits.

Bear in mind however, that currency with complete ID numbers would be in circulation, and complete correct ID numbers may therefore be copied one-for-one therefrom in large quantities over extended periods. But, if such sophisticated counterfeiting and preparation therefor was carefully committed over an extended period, archived currency flow information, as and if available, may reveal to authorities patterns of when and where authentic currency ID numbers copied from were situated in order for this copying to occur, thereby providing a possible lead for pursuers to follow.

Random and/or Secret Code

It may be useful in some counterfeit detection applications to provide ID numbers verifiable in some fashion in accord with a secret algorithm. For example, this may be accomplished according to applicants' invention as described above, i.e., to append to a serial number one or more distinct portions that conform to one or more respective secret codes. Such portions may be called secret code fields. In addition, random fields may or may not also be appended to the ID number.

In the first example, one secret code field is appended to the serial number (random fields are not used in this first example). The secret code field is represented by the ?? (the appended secret code field being undetermined thus far). The first example:

First example: 123456 ??

The second example uses two appended random fields (each random field has two randomly selected digits in these examples) and one appended secret code field (containing two digits that result from calculating a code in these examples) all three of which (fields) are used in a manner independent of each other. The secret code field is represented by the ?? (the appended secret code field being undetermined thus far). These three fields are shown in the second example as follows:

Second example: 123456 23 17 ??

The following technique may be employed to calculate the secret code field for both the first and second example. To the sum of the digits of the serial number portion add one, multiply by 541 and then divide by 11:

1+2+3+4+5+6=21+1=22.times.541=11,902+11.div.1082.0000

Do not use the result-only use two digits, the two digits located on either

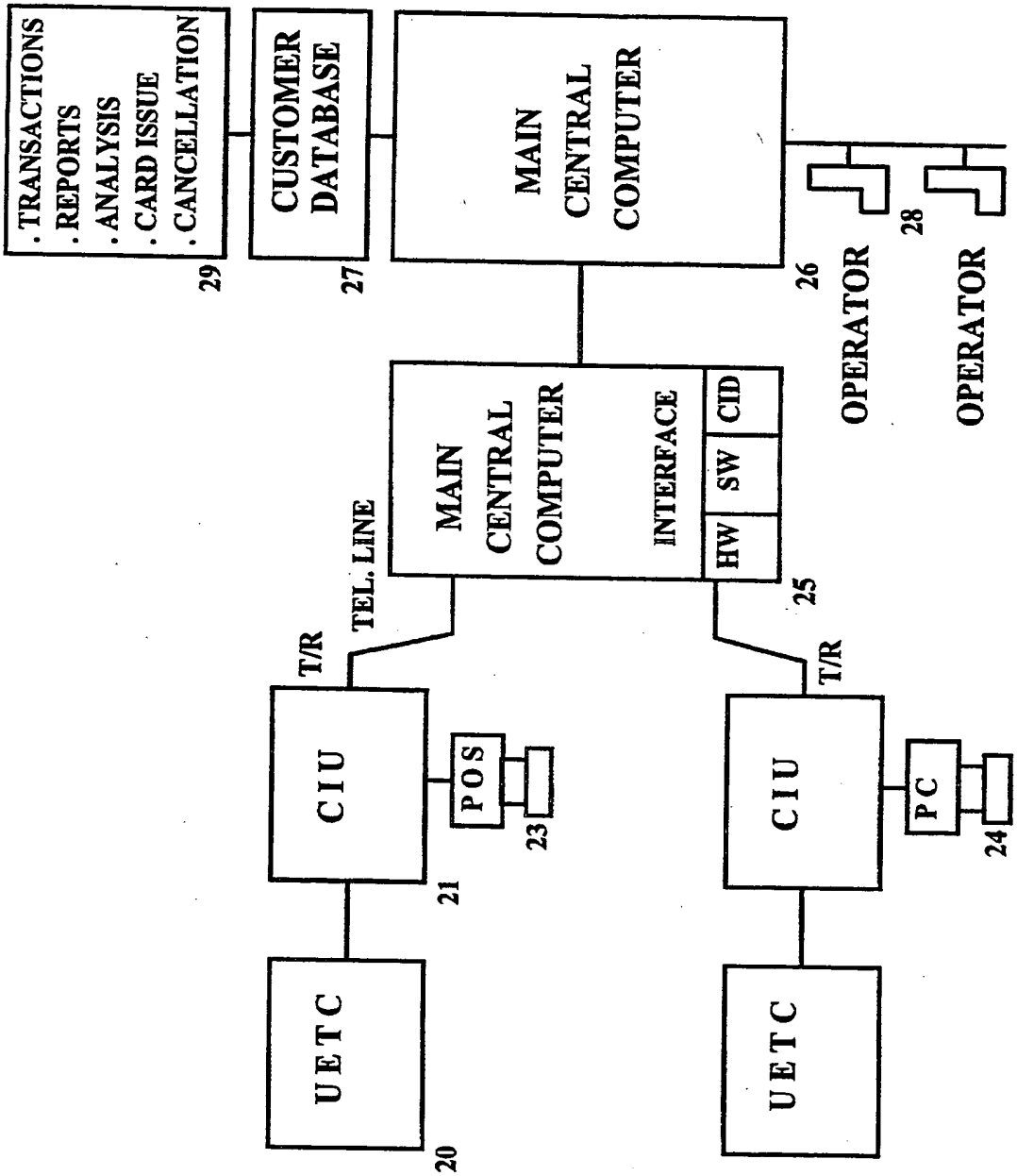
. TRANSACTIONS
. REPORTS
. ANALYSIS
. CARD ISSUE
. CANCELLATION
29
CUSTOMER DATABASE
27
MAIN CENTRAL COMPUTER
26
OPERATOR
28
OPERATOR
MAIN CENTRAL COMPUTER
INTERFACE
HW
SW
CID
25
TEL. LINE
T/R
T/R
CIU
21
POS
23
CIU
PC
24
UETC
20
UETC

FIG. 2